Structures mathématiques

Semestre d'hiver 2016/2017

Université du Luxembourg

Gabor Wiese[1]
gabor.wiese@uni.lu

Version du 24 septembre 2017

[1]Je remercie Agnès David pour sa collaboration à une version antérieure.

Table des matières

Préface

Les mathématiques à l'université sont différentes de ce qui est (habituellement) enseigné aux lycées : à l'université, le « comment est-ce que cela marche ? » est complété par « pourquoi est-ce que cela marche ? », « comment est-ce que cela se généralise ? », « quelle est l'idée principale derrière ? »
Dans vos cours de mathématiques à l'université, vous n'allez pas seulement apprendre comment on fait certains calculs, vous allez plutôt être introduits à des théories (j'aime bien appeler cela le « bâtiment des mathématiques ») qui donne lieu à des recettes de calculs, mais surtout à une compréhension approfondie d'un domaine.

Pour établir une théorie (pour la construction du bâtiment des mathématiques) il est essentiel de construire solidement. C'est pour cela que tout terme doit être défini (de façon à ne pas permettre d'ambiguïté) et toute assertion démontrée.
Le but de ce cours est que vous appreniez les fondations du langage mathématique et des techniques et structures de base. Cela est la condition sans laquelle les autres cours ne peuvent être compris.

Je vous souhaite beaucoup de plaisir à découvrir les mathématiques et un bon début de vos études !
Gabor Wiese

Littérature

Pour le début, qui est sans doute la partie la plus difficile, je recommande les livres suivants qui devraient être disponibles dans la bibliothèque au Kirchberg.

- Schichl, Steinbauer : *Einführung in das mathematische Arbeiten*.
- Scharlau : *Schulwissen Mathematik : Ein Überblick*, Vieweg, 3rd ed., 2001.
- Cramer : *Vorkurs Mathematik : Arbeitsbuch zum Studienbeginn in Bachelor-Studiengängen*, Springer, 2012.
- Fritzsche : *Mathematik für Einsteiger Spektrum*.

Voici quelques références pour des cours d'algèbre linéaires et introduction à l'algèbre qui traiterons ce que nous faisons et beaucoup plus : ces livres devraient également être disponibles dans la bibliothèque au Kirchberg.

- Lelong-Ferrand, Arnaudiès : *Cours de mathématiques, Tome 1, Algèbre*. Dunod. Ce livre est très complet et très détaillé. On peut l'utiliser comme ouvrage de référence.
- Siegfried Bosch : *Algebra* (en allemand), Springer-Verlag. Ce livre est très complet et bien lisible.
- Serge Lang : *Algebra* (en anglais), Springer-Verlag. C'est comme une encyclopédie de l'algèbre ; on y trouve beaucoup de sujets rassemblés, écrits de façon concise.
- Siegfried Bosch : *Lineare Algebra*, Springer-Verlag.
- Jens Carsten Jantzen, Joachim Schwermer : *Algebra*.
- Christian Karpfinger, Kurt Meyberg : *Algebra : Gruppen - Ringe - Körper*, Spektrum Akademischer Verlag.
- Gerd Fischer : *Lehrbuch der Algebra : Mit lebendigen Beispielen, ausführlichen Erläuterungen und zahlreichen Bildern*, Vieweg+Teubner Verlag.
- Gerd Fischer : *Lineare Algebra : Eine Einführung für Studienanfänger*, Vieweg+Teubner Verlag.

- Gerd Fischer, Florian Quiring : *Lernbuch Lineare Algebra und Analytische Geometrie : Das Wichtigste ausführlich für das Lehramts- und Bachelorstudium*, Springer Vieweg.
- Perrin : *Cours d'algèbre*, Ellipses.
- Guin, Hausberger : *Algèbre I. Groupes, corps et théorie de Galois*, EDP Sciences.
- Fresnel : *Algèbre des matrices*, Hermann.
- Tauvel : *Algèbre*.
- Combes : *Algèbre et géométrie*.
- Godement : *Cours d'algèbre*.

Chapitre I

Introduction aux mathématiques à l'université

1 Les démonstrations et les premiers mots du langage mathématique

Objectifs de cette section :

- Comprendre le concept de démonstration ;
- comprendre les concepts de définition, lemme, proposition, théorème ;
- faire connaissance avec des exemples de démonstrations directes et indirectes ;
- faire connaissance avec des exemples de définitions, lemmes, propositions, théorèmes ;
- maîtriser la manipulation d'équations simples ;
- maîtriser l'utilisation des indices, des sommes et des produits ;
- maîtriser les démonstrations par récurrence.

Une grande partie du contenu de cette section a déjà été traitée dans le cours de M. Schlenker pendant la semaine préparatoire. On donnera donc parfois moins de détails au cours.

Quelques mots au début – Aller Anfang ist schwer... und leicht

Le début des études de mathématiques est (comme Schichl et Steinbauer l'écrivent dans *Einführung in das mathematische Arbeiten*)

- **très difficile**, du fait de l'abstraction (définition, proposition, démonstration) et de l'utilisation d'un langage particulier, le langage mathématique,
- **facile**, car une grande partie des sujets a déjà été traitée au lycée.

Les mathématiques à l'université sont caractérisées par la **certitude absolue** de leurs résultats. Il ne suffit plus – comme souvent au lycée – d'expliquer un phénomème par beaucoup d'exemples ou d'apprendre une technique de calcul ; à l'université, il s'agit de le **démontrer**, c'est-à-dire d'écrire une **démonstration** (aussi appelée une **preuve**) qui, par une chaîne d'arguments faciles à suivre et compréhensibles pour tous, ne laisse aucun doute sur la vérité d'une assertion.
Pour pouvoir dire qu'une assertion est vraie avec une certitude absolue, il faut que tous les mots qui sont utilisés aient une signification très précise qui est la même pour tous. Par exemple, la phrase « La maison est haute » a certainement une signification différente pour quelqu'un de New York et pour quelqu'un venant d'un petit village en Sibérie.
Le langage mathématique diffère du langage du quotidien par :

- sa **précision**, tout terme a une définition précise ;
- son **formalisme**, souvent, on utilise des symboles et des formules.

Ce cours d'algèbre commencera donc par des exemples de preuves et l'introduction du langage mathématique.
On vous conseille fortement de vous **procurer des livres** (dans la bibliothèque sur support papier ou dans les répertoires électroniques) :

- spécialisés pour le grand pas entre l'école et l'université (comme Schichl/Steinbauer : *Einführung in das mathematische Arbeiten*) ;
- d'introduction à l'algèbre et à l'algèbre linéaire.

Un mot d'explication sur « l'algèbre » et « l'algèbre linéaire » : à l'Université du Luxembourg, ces deux cours sont enseignés au premier semestre, tandis qu'en France et en Allemagne, les cours d'algèbre ne commencent qu'en deuxième année et reposent sur les cours d'algèbre linéaire. Ne soyez pas choqués par ce fait (mais gardez-le à l'esprit quand vous regardez des livres – il vous faut aussi des livres sur l'algèbre linéaire). Le cours d'algèbre linéaire à l'UL est en commun avec d'autres filières du Bachelor et le cours d'algèbre est destiné uniquement aux étudiants en mathématiques. En cours d'algèbre, nous allons faire une grande partie de ce qui se fait habituellement dans les cours d'algèbre linéaire dans d'autres pays, sauf que vous allez très bien vous entraîner aux calculs importants de matrices dans votre cours d'algèbre linéaire ; cela nous permettra d'aller un tout petit peu plus loin que l'algèbre linéaire dans notre cours.

Définition, proposition, démonstration

On utilise les notations suivantes (connues de l'école) :

- $\mathbb{N}$, les entiers naturels : $0, 1, 2, 3, \ldots$;
- $\mathbb{Z}$, les entiers relatifs : $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$;
- $\mathbb{Q}$, les nombres rationnels ;
- $\mathbb{R}$, les nombres réels ;

- $\mathbb{C}$, les nombres complexes.

On rappelle la notion de *divisibilité* dans les entiers relatifs. On dit qu'un entier relatif $q \neq 0$ divise un entier relatif n (et que q est un diviseur de n) si le reste de la division de n par q est zéro, ou, dit autrement, s'il existe un entier relatif m tel que $n = mq$.
En fait, les phrases précédentes signifient que nous avons donné un nom (« diviseur ») à une propriété mathématique. C'est un exemple de **définition**. Pour souligner le rôle essentiel des définitions en mathématiques, nous les formulons comme suit.

Définition 1.1. *Soient $n, q \in \mathbb{Z}$.*
On dit que q est un diviseur *de n et que q* divise *n s'il existe $m \in \mathbb{Z}$ tel que*

$$n = mq.$$

On utilise le symbole $q \mid n$ pour signifier que q divise n.

Définition 1.2. *Soit $n \in \mathbb{Z}$. On dit que n est* pair *si 2 divise n (en symboles : $2 \mid n$).*

Une définition n'est pas vraie ou fausse. C'est seulement un nom qu'on donne à une propriété pour pouvoir mieux l'utiliser. Mais les définitions sont d'une importance fondamentale pour les mathématiques parce qu'elles « définissent » les objets avec lesquels nous allons travailler, donc sur lesquels nos propositions vont porter.

Proposition 1.3. *Le carré d'un nombre pair est pair.*

Vocabulaire :

- Une **proposition** est une assertion qui est vraie avec une certitude absolue, c'est-à-dire qui a été démontrée.
- Un **théorème** est un autre mot pour une assertion qui est vraie avec une certitude absolue. On utilise habituellement le mot « théorème » pour les assertions les plus importantes.
- Un **lemme** est encore un autre mot pour une assertion qui est vraie avec une certitude absolue. Les lemmes ont souvent une fonction secondaire et auxiliaire ; on les utilise pour démontrer des propositions ou des théorèmes.
- Un **corollaire** est encore un autre mot pour désigner une assertion. On l'utilise pour des énoncés qui se déduisent facilement d'un autre résultat, en général une proposition ou un théorème. Le contenu d'un corollaire peut être très important, mais sa démonstration à partir de la proposition ou du théorème initial est rapide.

Démonstration de la proposition 1.3. Soit $n \in \mathbb{Z}$ pair. D'après les définitions précédentes, cela veut dire qu'il existe $m \in \mathbb{Z}$ tel que

$$n = 2m.$$

Cela implique que

$$n^2 = (2m)^2 = 4m^2.$$

Donc

$$n^2 = 2 \cdot (2m^2).$$

Alors, n^2 est divisible par 2, donc pair. □

Cette démonstration est la première dans ce cours. On voit que c'est une suite d'arguments, et chaque étape est facile à vérifier pour tous. Donc, on peut en effet dire que la proposition est vraie avec une certitude absolue.
Cette preuve est un exemple d'une **démonstration directe** : nous avons commencé par **l'hypothèse** (n est un entier relatif pair) et nous avons terminé par l'assertion recherchée.
Il est habituel de signaler la fin d'une preuve par un symbole spécial ou par une abbréviation standard. La fin des preuves dans ces notes sera toujours marquée par le symbole □. D'autres professeurs utilisent d'autres symboles. Une abbréviation très courante est « q.e.d. » (quod erat demonstrandum – ce qui a été à démontrer).

Voici une autre définition.

Définition 1.4. *Un entier relatif $p \in \mathbb{Z}$ est appelé* nombre premier *si $p > 1$ et les seuls diviseurs positifs de p sont 1 et p.*

Nous avons donné cette définition et maintenant nous voulons en savoir autant que possible sur cette nouvelle notion que nous avons définie. Pour commencer, les nombres premiers inférieurs à 20 sont : 2, 3, 5, 7, 11, 13, 17, 19. Vous connaissez certainement d'autres nombres premiers. Une question vient donc immédiatement à l'esprit : existe-t-il une infinité de nombres premiers ?
La réponse a déjà été donnée par Euclide il y a plus de 2200 ans.

Théorème 1.5 (Euclide)**.** *Il existe une infinité de nombres premiers.*

La démonstration donnée par Euclide est souvent considérée comme l'exemple d'une preuve belle et élégante. C'est une **démonstration indirecte** ou, plus précisement, **démonstration par l'absurde**. On donne d'abord la démonstration et on expliquera ces termes juste après.

Démonstration. Supposons pour l'instant le contraire de ce que nous voulons démontrer : il n'existe qu'un nombre fini (disons n) de nombres premiers. On peut alors les numéroter :

$$p_1, p_2, p_3, \ldots, p_n.$$

Considérons l'entier positif

$$m := p_1 p_2 p_3 \cdots p_n + 1. \tag{1.1}$$

Nous allons maintenant utiliser le fait que tout entier positif ≥ 2 s'écrit comme produit de nombres premiers. Cette assertion doit être démontrée ! Nous le faisons dans le lemme 1.6 qui suit.
Il existe alors un nombre premier p qui divise m. Le nombre premier p doit appartenir à notre liste complète des nombres premiers, donc $p = p_i$ pour un certain i entre 1 et n.
L'équation (1.1) montre que la division de m par p_i laisse le reste 1.
Nous avons trouvé qu'en même temps p_i divise m et laisse le reste 1. Ceci est **absurde**, c'est une **contradiction**.
Donc, notre hypothèse faite au début de cette preuve ne peut pas être vraie. Alors, son contraire est vrai : il existe une infinité de nombres premiers. □

Le principe de cette preuve indirecte est de supposer vrai le contraire de l'assertion recherchée. Puis, on donne une suite d'arguments, comme avant, pour arriver à une assertion, dont on sait qu'elle est fausse, **absurde** et **contradictoire** (dans notre preuve : le reste de la division de m par p est à la fois 0 et 1). Nous savons alors que le contraire de l'assertion recherchée est faux. Cela signifie que l'assertion est vraie, car une assertion est soit vraie soit fausse. Ce fait est souvent écrit en latin « Tertium non datur » et s'appelle en français « Principe du tiers exclu ». On en reparlera plus tard.

Lemme 1.6. *Soit $n \geq 2$ un entier relatif. Alors il existe des nombres premiers $p_1, \ldots, p_k$ tels que*

$$n = p_1 p_2 \cdots p_k.$$

Remarquons que dans l'énoncé du lemme, les nombres premiers ne sont pas nécessairement distincts. Remarquons également que, pour être encore plus précis, on aurait du écrire : « Alors il existe un entier $k \geq 1$ et il existe des nombres premiers $p_1, \ldots, p_k$ tels que $n = p_1 p_2 \cdots p_k$ ». Il est habituel de formuler l'enoncé comme nous l'avons fait, mais il faut toujours être conscient que l'existence de k est implicite.
La preuve de ce lemme est un autre exemple d'une démonstration par l'absurde.

Démonstration (par l'absurde). Supposons que l'énoncé du lemme est faux. Dans ce cas, il existe un entier positif ≥ 2 qui ne s'écrit pas comme un produit de nombres premiers. Soit n le plus petit entier ayant cette propriété.
Nous distinguons des cas.
1er cas : n est premier. Dans ce cas, on prend $k = 1$ et $p_1 = n$, donc on a $n = p_1$.
2ème cas : n n'est pas un nombre premier. Alors, n possède un diviseur positif d différent de 1 et n. Par définition (de diviseur) il existe $m \in \mathbb{Z}$ tel que

$$n = md.$$

Notons que $1 < d < n$ et $1 < m < n$.
Comme n est le plus petit entier positif qui ne s'écrit pas comme un produit de nombres premiers et m, d sont strictement plus petits, ces deux nombres s'écrivent sous la forme

$$m = p_1 p_2 \cdots p_k \quad \text{et} \quad d = q_1 q_2 \cdots q_\ell$$

avec des nombres premiers $p_1, \ldots, p_k$ et $q_1, \ldots, q_\ell$.
Cela donne :

$$n = md = p_1 p_2 \cdots p_k q_1 q_2 \cdots q_\ell.$$

Nous avons donc obtenu que n s'écrit comme produit de nombres premiers. Ceci contredit notre hypothèse que l'énoncé du lemme est faux. Alors, c'est faux que le lemme est faux ; donc, le lemme est vrai. □

Assertions

Nous allons regarder la structure des écrits mathématiques de plus près. Le rôle central est occupé par les assertions. Par exemple, une preuve est une suite d'assertions de telle sorte que la **vérité** d'une assertion **implique** la vérité de l'assertion suivante.

Une **assertion** est une phrase (en mathématiques, ou ailleurs) qui est **soit vraie**, **soit fausse**, mais pas les deux en même temps.[1]

Il n'y a donc pas de troisième possibilité (en latin : *tertium non datur*). Nous avons déjà vu des exemples :

- *Le carré d'un entier relatif pair est pair.*

  Cette assertion est vraie comme nous l'avons vu dans la proposition 1.3.

- *Il n'y a qu'un nombre fini de nombres premiers.*

  Cette assertion est fausse (voir le théorème 1.5).

D'autres exemples d'assertions :

- $x = 1$

  La véracité ou non de cette assertion dépend du contexte, car nous n'avons pas précisé ce qu'était x.

  - Soit x une solution de l'équation $2x = 2$. Dans ce contexte, l'assertion « $x = 1$ » est vraie (on le démontre en divisant par 2).
  - Soit x une solution de l'équation $2x = 4$. Dans ce contexte, l'assertion « $x = 1$ » est fausse.
  - Soit x une solution de l'équation $x^2 = 1$. Dans ce contexte, nous ne pouvons rien dire quant à la vérité de l'assertion « $x = 1$ » car x peut être 1 ou -1.

- Pour illustrer, on peut aussi prendre des assertions de notre vie quotidienne, par exemple :

  - Il pleut.
  - La rue est mouillée.
  - etc.

Implication

Si la véracité d'une assertion entraîne celle d'une autre, on parle d'une *implication* que nous notons $\Rightarrow$ (ou $\Leftarrow$ selon la situation). Le symbole $\Rightarrow$ se lit comme : « implique », « alors », « en conséquence », « donc », « est suffisant pour » etc. Nous allons formaliser ces concepts dans la prochaine section ; maintenant nous allons regarder des exemples.

(1) Assertion A : « Il pleut. »

Assertion B : « La rue est mouillée. »

Nous pouvons les combiner pour obtenir l'assertion :
« S'il pleut, alors la rue est mouillée. »
En symboles : Il pleut. $\Rightarrow$ La rue est mouillée.

[1] Il y a des subtilités concernant cette phrase que nous n'évoquerons pas (il faut que l'assertion soit formulée convenablement) car vous ne les rencontrerez dans aucun cours de vos études, sauf si vous suivez un cours de logique mathématique.

Cette assertion est certainement vraie. Notez que nous n'avons pas dit que l'assertion A est vraie. Nous avons seulement fait une remarque sur la *relation* entre les deux assertions. Cela ne devrait pas vous choquer : La phrase « S'il pleut, alors la rue est mouillée. » est vraie même s'il ne pleut pas en ce moment.

On peut aussi écrire la même chose comme ça :
La rue est mouillée. $\Leftarrow$ Il pleut.

Nous avons donc seulement échangé les deux côtés, mais le contenu reste le même. En mots, on pourrait dire :
« La rue est mouillée s'il pleut. »

Voici une formulation plus sophistiquée pour encore dire la même chose :
« Il suffit qu'il pleuve pour que la rue soit mouillée. »

Noter que l'assertion
« Si la rue est mouillée, il pleut. »
est fausse car il peut y avoir d'autres raisons pour une rue mouillée (par ex., lavage).

(2) Assertion A : « Je réussis l'examen. »

Assertion B : « Je reçois les points ECTS. »

On peut les combiner ainsi :
« Si je réussis l'examen, alors je reçois les points ECTS. »
en symboles : Je réussis l'examen. $\Rightarrow$ Je reçois les points ECTS.

C'est également une assertion vraie.

(3) Assertion A : « $x = 1$ »

Assertion B : « $2x = 2$ »

Nouvelle assertion vraie : « $x = 1 \Rightarrow 2x = 2.$ »
On pourrait aussi écrire : « $2x = 2 \Leftarrow x = 1.$ »

Répétons que nous n'avons rien dit sur la vérité des assertions A et B. Nous avons seulement constaté une relation entre les deux assertions.

(4) Assertion A : « $x = 1$ »

Assertion B : « $x^2 = 1$ »

Nouvelle assertion vraie : « $x = 1 \Rightarrow x^2 = 1.$ »
On pourrait aussi écrire : « $x^2 = 1 \Leftarrow x = 1.$ »

(5) (Juste pour montrer qu'on peut aussi obtenir des assertions fausses :)

Assertion A : « $x = 1$ »

Assertion B : « $2x = 4$ »

Nouvelle assertion (fausse !) : « $x = 1 \Rightarrow 2x = 4.$ »

« $A \Rightarrow B$ » et « $A \Leftarrow B$ » doivent être bien distingués !

Voici un exemple d'une utilisation incorrecte :

S'il fait nuit, alors les phares des voitures sont allumés. Les phares de cette voiture sont allumés, donc il fait nuit.

Equivalence

Si une assertion est vraie si et seulement si une autre est vraie, on parle de *l'équivalence* des deux assertions, notée $\Leftrightarrow$. Le symbole $\Leftrightarrow$ indique l'équivalence ; il veut dire que les deux implications $\Rightarrow$ et $\Leftarrow$ sont vraies en même temps. Il se dit « est équivalent à », « si et seulement si », etc.
Exemples :

(1) Je reçois les points ECTS si et seulement si je réussis l'examen.
En symboles : Je reçois les points ECTS. $\Leftrightarrow$ Je réussis l'examen.

(2) Soit x un nombre réel. On a $2x = 2$, si et seulement si $x = 1$.
En symboles : $2x = 2 \ \Leftrightarrow \ x = 1$

(3) Soit x un nombre réel. On a $x^2 = 1$, si et seulement si $x = 1$ ou $x = -1$.
En symboles : $x^2 = 1 \ \Leftrightarrow \ (x = 1$ ou $x = -1)$

Discutons d'abord pourquoi il n'y a pas d'exemple avec une rue mouillée : L'assertion : « La rue est mouillée. $\Rightarrow$ Il pleut. » est fausse (car quelqu'un pourrait nettoyer sa voiture) ! Alors, il ne s'agit pas d'une équivalence. Aussi l'assertion : « $x^2 = 1 \Leftrightarrow x = 1$ » est fausse, car l'assertion « $x^2 = 1 \Rightarrow x = 1$ » est fausse, parce que $x = -1$ est une autre solution.
Voici un autre exemple de proposition.

Proposition 1.7. *Soient n, m des entiers relatifs. Alors les assertions suivantes sont équivalentes :*

(i) n *est pair.*

(ii) $n + 2m$ *est pair.*

Si on démontre une équivalence, il faut démontrer les deux assertions $\Rightarrow$ et $\Leftarrow$.

Démonstration. « (i) $\Rightarrow$ (ii) » : On suppose que (i) est vrai : que n est pair. Il existe donc $q \in \mathbb{Z}$ tel que $n = 2q$. Alors, $n + 2m = 2q + 2m = 2(q + m)$. Donc $n + 2m$ est pair.
« (i) $\Leftarrow$ (ii) » : On suppose que (ii) est vrai : $n + 2m$ est pair. Il existe donc $q \in \mathbb{Z}$ tel que $n + 2m = 2q$. Alors, $n = 2q - 2m = 2(q - m)$. Donc n est pair. □

Comment manipuler des équations

On commence cette petite partie par un avertissement :

Faites bien attention au symbole $\Rightarrow$, $\Leftarrow$, $\Leftrightarrow$ à utiliser.

C'est une grande source d'erreur au début.
Nous allons insister sur l'utilisation des symboles $\Rightarrow$, $\Leftarrow$, $\Leftrightarrow$ dans les manipulations des équations.

Voici un exemple. Soit x un nombre réel.

$$\begin{array}{lrl} & x^2+3=4x-1 & |-(4x-1) \\ \Rightarrow & x^2-4x+4=0 & \\ \Rightarrow & (x-2)^2=0 & |\sqrt{\ } \\ \Rightarrow & x-2=0 & |+2 \\ \Rightarrow & x=2 & \end{array}$$

Notre calcul montre : si $x \in \mathbb{R}$ est une solution de l'égalité $x^2+3=4x-1$, alors $x=2$. Elle ne montre pas que $x=2$ est une solution. Mais cette dernière assertion est aussi correcte : $2^2+3=4\cdot 2-1$. Nous pouvons rajouter une autre ligne en bas de notre calcul :

$$\Rightarrow x^2+3=4x-1.$$

Nous avons fermé le cercle : on peut déduire de la vérité de n'importe laquelle des assertions dans le calcul la vérité des autres en suivant les flèches d'implication. Donc, toutes les manipulations que nous avons faites sont en effet des équivalences : on aurait pu écrire $\Leftrightarrow$ au lieu de $\Rightarrow$ à chaque fois. On pourrait aussi vérifier que chacune des implications que nous avons écrites est en fait une équivalence. Vous pensez peut-être que les remarques précédentes ne sont que des subtilités sans importance. Considérons encore une fois un nombre réel x et faisons le calcul suivant :

$$\begin{array}{lrl} & x^2=-9 & |\text{ carré} \\ \Rightarrow & x^4=81 & |\sqrt[4]{\ } \\ \Rightarrow & x=3 \text{ ou } x=-3 & \end{array}$$

Les manipulations sont correctes et ce calcul montre : si $x \in \mathbb{R}$ est une solution de l'égalité $x^2=-9$, alors $x=3$ ou $x=-3$. Mais, ni l'un ni l'autre n'est une solution de l'équation de départ ! Pourquoi ? Parce que notre équation du début ne possède aucune solution dans $\mathbb{R}$. Donc, attention à vérifier que vos calculs donnent une solution au problème initial.

Que pensez-vous des arguments suivants ? Soient n, m deux nombres réels.

$$\begin{array}{lrl} & n=m & |\cdot n \\ \Rightarrow & n^2=nm & |+n^2 \\ \Rightarrow & n^2+n^2=n^2+nm & \\ \Rightarrow & 2n^2=n^2+nm & |-2nm \\ \Rightarrow & 2n^2-2nm=n^2+nm-2nm & \\ \Rightarrow & 2n^2-2nm=n^2-nm & \\ \Rightarrow & 2(n^2-nm)=1\cdot(n^2-nm) & |:(n^2-nm) \\ \Rightarrow & 2=1 & \end{array}$$

Nous avons donc démontré : Si $n=m$, alors $2=1$. L'égalité $n=m$ peut être facilement satisfaite, par exemple par $n=m=1$. Alors l'assertion $2=1$ est vraie. Quoi ? ? ? ? ? ? ?

La faute se passe dans la dernière implication. Elle est fausse si $n^2 - nm = 0$ (c'est d'ailleurs le cas quand $n = m$), parce que dans ce cas, nous divisons par zéro. Notez que quelle que soit la valeur de $n^2 - nm$, multiplier par cette expression donne une implication :

$$a(n^2 - nm) = b(n^2 - nm) \Leftarrow a = b.$$

Nous avons donc mis $\Rightarrow$ où $\Leftarrow$ aurait été correct. Mais $\Leftarrow$ dans la dernière ligne ne nous permet plus de déduire que l'assertion $2 = 1$ est vraie. Ouf, sauvés.

Encore un autre... Soient n, m deux nombres réels.

$$\begin{aligned}
& m = n + 1 && | - m \\
\Rightarrow \quad & 0 = n + 1 - m && | \cdot 4 \\
\Rightarrow \quad & 0 = 4n + 4 - 4m && | + (n^2 - 2mn + m^2) \\
\Rightarrow \quad & n^2 - 2mn + m^2 = n^2 + 4n + 4 - 2mn - 4m + m^2 && \\
\Rightarrow \quad & (n - m)^2 = (n + 2)^2 - 2(n + 2)m + m^2 && \\
\Rightarrow \quad & (n - m)^2 = (n + 2 - m)^2 && |\sqrt{\ } \\
\Rightarrow \quad & n - m = n + 2 - m && | + (m - n) \\
\Rightarrow \quad & 0 = 2 &&
\end{aligned}$$

Nous avons donc démontré : Si $m = n + 1$, alors $0 = 2$. L'égalité $m = n + 1$ peut être facilement satisfaite, par exemple par $m = 1$ et $n = 0$. Alors l'assertion $0 = 2$ est vraie. Nous avons donc encore une fois « démontré » une assertion évidement fausse. Pourquoi ? ? ? ? ?

Indices, sommes et produits

Si nous avons une fonction qui dépend de deux variables, par exemple $f(x, y) = x^2 + 2y$, on peut les numéroter en utilisant des indices x_1, x_2 (dans notre exemple : $f(x_1, x_2) = x_1^2 + 2x_2$). Cela est surtout utile si le nombre des variables n'est pas fixe, par exemple $f(x_1, x_2, \ldots, x_n)$. Nous avons aussi déjà utilisé des indices dans les sections précédentes, par ex. $p_1, p_2, \ldots, p_n$.
Vous connaissez peut-être aussi les polynômes. Un polynôme de degré n à coefficients rationnels est une expression :

$$p(x) = a_0 x^0 + a_1 x^1 + a_2 x^2 + \cdots + a_n x^n$$

avec $a_0, a_1, \ldots, a_n \in \mathbb{Q}$ et $a_n \neq 0$ (pour que le degré soit vraiment n et pas inférieur). Évidemment, on peut faire la même chose pour des coefficients dans un autre ensemble que $\mathbb{Q}$ (par exemple $\mathbb{R}$ ou $\mathbb{C}$).
Il est possible d'avoir deux indices. Par exemple, on peut numéroter les entrées d'une matrice A de taille $n \times m$ comme suit :

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \ldots & a_{1,m} \\ a_{2,1} & a_{2,2} & a_{2,3} & \ldots & a_{2,m} \\ a_{3,1} & a_{3,2} & a_{3,3} & \ldots & a_{3,m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & a_{n,3} & \ldots & a_{n,m} \end{pmatrix}.$$

On peut, par exemple, définir une matrice de taille 3×3 par la formule :

$$a_{i,j} := 3 \cdot (i-1) + j \text{ pour } 1 \leq i \leq 3 \text{ et } 1 \leq j \leq 3.$$

Cela donne

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}.$$

Il peut même nous arriver d'avoir des indices qui ont aussi des indices eux-mêmes, par exemple :
$A_{1,1}, A_{1,2}, \dots A_{1,e_1}$
$A_{2,1}, A_{2,2}, \dots A_{2,e_2}$
$\dots$
$A_{n,1}, A_{n,2}, \dots A_{n,e_n}$
On peut imaginer cet exemple comme une matrice, sauf que la longueur des lignes varie d'une ligne à l'autre.

Définition 1.8. *Le symbole* delta de Kronecker *est défini comme*

$$\delta_{i,j} = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

Par exemple, nous avons pour $n \in \mathbb{N}$

$$A = \begin{pmatrix} \delta_{1,1} & \delta_{1,2} & \delta_{1,3} & \dots & \delta_{1,n} \\ \delta_{2,1} & \delta_{2,2} & \delta_{2,3} & \dots & \delta_{2,n} \\ \delta_{3,1} & \delta_{3,2} & \delta_{3,3} & \dots & \delta_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \delta_{n,1} & \delta_{n,2} & \delta_{n,3} & \dots & \delta_{n,n} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix},$$

c'est la matrice « identité ».

Nous avons souvent utilisé les trois points « $\dots$ ». C'est une écriture suggestive, mais pas précise ! Vous pensez que $3, 5, 7, \dots$ est la suite des nombres impairs supérieurs ou égaux à 3 ? Mais non, on pourrait aussi vouloir parler des nombres premiers impairs. Donc, il vaut mieux être précis. Pour cela on introduit les symboles $\sum$ et $\prod$ pour les sommes et les produits.
Voici des exemples :

- Notre polynôme ci-dessus s'écrit :

$$p(x) = a_0 x^0 + a_1 x^1 + a_2 x^2 + \cdots + a_n x^n = \sum_{i=0}^{n} a_i x^i.$$

  Cette notation dit que l'indice i parcourt les $n+1$ entiers entre 0 et n (avec 0 et n inclus).

- $\sum_{i=1}^{5} i = 1 + 2 + 3 + 4 + 5 = 15.$
- $\prod_{i=1}^{5} i = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120.$

- $\sum_{i=1}^{5} i^2 = 1^2 + 2^2 + 3^2 + 4^2 + 5^2 = 55$.
- $\prod_{i=1}^{5} i^2 = 1^2 \cdot 2^2 \cdot 3^2 \cdot 4^2 \cdot 5^2 = 14400$.
- Cas spécial de la somme vide : Soient $b < a$ des entiers relatifs. Alors

$$\sum_{i=a}^{b} a_i = 0$$

  pour n'importe quel a_i.

- Cas spécial du produit vide : Soient $b < a$ des entiers relatifs. Alors

$$\prod_{i=a}^{b} a_i = 1$$

  pour n'importe quel a_i.

Définition 1.9. *Pour un entier naturel n on définit n* factorielle *comme*

$$n! = \prod_{i=1}^{n} i.$$

Noter le cas spécial $0! = 1$ qui correspond au produit vide. Nous avons déjà vu le cas spécial $5! = 120$ plus haut.

Récurrence

Une méthode de preuve très souvent utilisée est la **démonstration par récurrence**. Nous commençons par un exemple qui – selon la légende – est dû à Gauß quand il était enfant. Son professeur voulait occuper les enfants et leur a demandé de calculer la somme des entiers naturels jusqu'à 100, c'est-à-dire $1 + 2 + \cdots + 100 = \sum_{i=1}^{100} i$. Gauß a trouvé la réponse tout de suite : 5050. On peut s'imaginer que son professeur n'était pas content car il lui fallait alors trouver d'autres choses pour occuper les enfants.

Proposition 1.10 (« Petit Gauß »)**.** *Pour tout nombre naturel $n \geq 1$, on a la formule :*

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Démonstration.

(1) On commence toujours par une vérification de la formule au cas minimal, ici $n = 1$:

$$\sum_{i=1}^{1} i = 1 \overset{!}{=} \frac{1(1+1)}{2}.$$

(2) Supposons que nous savons déjà que la formule est vraie pour $n = m$ (par ex. $m = 1$). Nous allons la démontrer pour $n = m + 1$:

$$\sum_{i=1}^{m+1} i = \big(\sum_{i=1}^{m} i\big) + (m+1) \overset{\text{cas} n=m}{=} \frac{m(m+1)}{2} + (m+1)$$
$$= \frac{m(m+1) + 2(m+1)}{2} = \frac{(m+1)(m+2)}{2}.$$

(3) Ce que nous avons fait suffit déjà pour conclure que la formule est vraie pour tout $n \geq 1$:

Pour le cas $n = 1$ on utilise (1).
Puis on utilise (2) pour conclure du cas $n = 1$ le cas $n = 1 + 1 = 2$.
Puis on utilise (2) pour conclure du cas $n = 2$ le cas $n = 2 + 1 = 3$.
Puis on utilise (2) pour conclure du cas $n = 3$ le cas $n = 3 + 1 = 4$.
On se convainc que par ce processus on traite tous les $n \geq 1$.

□

Le principe de la démonstration précédente s'appelle « démonstration par récurrence ».
Nous formalisons ce principe maintenant. Soit $A(n)$ une assertion (pour n un entier), par exemple

$$A(n) : \ 1 + 2 + \cdots + n = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

Les trois étapes dans la preuve sont appelées ainsi :

Initialisation Démontrer que l'assertion $A(0)$ est vraie.

Hérédité Pour tout n dans $\mathbb{N}$, démontrer que l'assertion $A(n)$ implique l'assertion $A(n+1)$.

Conclusion Pour tout n dans $\mathbb{N}$, l'assertion $A(n)$ est vraie.

Un autre exemple :

Proposition 1.11 (Somme des premiers nombres impairs)**.** *Pour tout nombre naturel $n \geq 1$, on a la formule*

$$1 + 3 + 5 + \cdots + (2n-1) = \sum_{i=1}^{n} (2i-1) = n^2.$$

Démonstration. Nous voulons démontrer l'assertion

$$A(n) : \ 1 + 3 + 5 + \cdots + (2n-1) = \sum_{i=1}^{n} (2i-1) = n^2$$

pour tout nombre naturel $n \geq 1$.

Initialisation : Pour $n = 1$ on a $1 = 1^2$, donc $A(1)$ est vraie.

Hérédité : « $A(n) \Rightarrow A(n+1)$ » : Supposons donc que pour $n \in \mathbb{N}$ l'assertion $A(n)$ est vraie.

$$\sum_{i=1}^{n+1}(2i-1) = \big(\sum_{i=1}^{n}(2i-1)\big) + (2n+1) \overset{A(n)}{=} n^2 + (2n+1) = (n+1)^2,$$

donc $A(n+1)$ est vraie.

Conclusion : Pour tout $n \in \mathbb{N}_{>0}$ on a $\sum_{i=1}^{n}(2i-1) = n^2$.

□

Pour simplifier, nous allons utiliser les notations suivantes.

Notation 1.12. *Soit n_0 un entier naturel ; on note $\mathbb{N}_{\geq n_0}$ l'ensemble des entiers naturels supérieurs ou égaux à n_0 et $\mathbb{N}_{>n_0}$ l'ensemble des entiers naturels strictement supérieurs à n_0.*

Le principe de récurrence a plusieurs variantes.

Proposition 1.13 (Variantes du principe de récurrence)**.**

Changement d'initialisation *Soient n_0 dans $\mathbb{N}$ et, pour tout n dans $\mathbb{N}$ supérieur ou égal à n_0, une assertion $A(n)$. Alors :*

$$(A(n_0) \wedge (\forall n \in \mathbb{N}_{\geq n_0}, A(n) \Rightarrow A(n+1))) \Rightarrow (\forall n \in \mathbb{N}_{\geq n_0}, A(n)).$$

Récurrence forte *Soit, pour tout n dans $\mathbb{N}$, une assertion $A(n)$. Alors*

$$(A(0) \wedge (\forall n \in \mathbb{N}, (A(0) \text{ et } A(1) \dots \text{ et } A(n)) \Rightarrow A(n+1))) \Rightarrow (\forall n \in \mathbb{N}, A(n)).$$

Récurrence finie *Soient N et M dans $\mathbb{N}$, avec $N < M$ et pour tout entier n dans $\{N, \dots, M\}$, une assertion $A(n)$. Alors*

$$(A(N) \wedge (\forall n \in \{N, \dots, M-1\}, A(n) \Rightarrow A(n+1))) \Rightarrow (\forall n \in \{N, \dots, M\}, A(n)).$$

Récurrence finie descendante *Soient N et M dans $\mathbb{N}$, avec $N < M$ et pour tout entier n dans $\{N, \dots, M\}$, une assertion $A(n)$. Alors*

$$(A(M) \wedge (\forall n \in \{N+1, \dots, M\}, A(n) \Rightarrow A(n-1))) \Rightarrow (\forall n \in \{N, \dots, M\}, A(n)).$$

Développement du binôme de Newton

Définition 1.14. *Soient $n \in \mathbb{N}$ et $k \in \mathbb{Z}$ Pour $0 \leq k \leq n$, nous définissons le* coefficient binomial *comme*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Pour $k > n$ ou $k < 0$ on définit

$$\binom{n}{k} = 0.$$

En allemand on prononce : « n über k » ou « k aus n ». En anglais on dit : « n choose k ». En français on note aussi C_n^k (pour « combinaison de n parmi k »).

Exemple 1.15.

- *Pour tout n dans $\mathbb{N}$, on a* $\binom{n}{0} = \binom{n}{n} = 1$.
- *Pour tout n dans $\mathbb{N}_{>0}$, on a* $\binom{n}{1} = \binom{n}{n-1} = n$.

Lemme 1.16. *Pour $n, k \in \mathbb{N}$ et $k \leq n$ nous avons :*

$$\binom{n}{k} = \binom{n}{n-k}.$$

Lemme 1.17. *Pour $n, k \in \mathbb{N}$ et $k \leq n$ nous avons :*

$$\binom{n}{k} = \prod_{i=1}^{k} \frac{n+1-i}{i}.$$

Démonstration. Exercice. □

Proposition 1.18 (Formule de Pascal)**.** *Pour tout $k, n \in \mathbb{N}$ on a :*

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}.$$

Démonstration. On vérifie immédiatement l'égalité recherchée si $k \leq 0$ ou $k > n$. On peut donc supposer $1 \leq k \leq n$. La formule se vérifie par le calcul suivant :

$$\begin{aligned}
\binom{n}{k} + \binom{n}{k-1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} \\
&= \frac{n!(n+1-k)}{k!(n+1-k)!} + \frac{n!k}{k!(n+1-k)!} \\
&= \frac{n!(n+1-k+k)}{k!(n+1-k)!} \\
&= \frac{(n+1)!}{k!(n+1-k)!} \\
&= \binom{n+1}{k}.
\end{aligned}$$

□

Nous donnons maintenant l'explication combinatoire du coefficient binomial.

Proposition 1.19. *Pour tous n et k dans $\mathbb{N}_{\geq 1}$, le coefficient binomial* $\binom{n}{k}$ *exprime le nombre de possibilités pour choisir k entiers parmi $1, 2, \ldots, n$ (l'ordre ne jouant aucun rôle).*

Démonstration. Par récurrence sur n.

Initialisation : Pour $n = 1$ et $k = 1$ il n'existe qu'une seule possibilité et $\binom{1}{1} = 1$, donc l'assertion est vraie.

Hérédité : « $n \Rightarrow n+1$ » : On cherche à sélectionner k entiers parmi $1, \ldots, n+1$. On distingue selon deux cas : soit on sélectionne $n+1$, soit on ne le sélectionne pas.

Si on choisit $n+1$, il nous reste $k-1$ entiers à choisir, parmi $1, \ldots, n$. Par hypothèse de récurrence, il existe $\binom{n}{k-1}$ possibilités de choisir $k-1$ nombres parmi $1, 2, \ldots, n$. Donc, il existe $\binom{n}{k-1}$ possibilités de choisir k éléments parmi $1, 2, \ldots, n+1$ à la condition que $n+1$ est choisi.

Si on ne choisit pas $n+1$, cela signifie qu'on va choisir nos k entiers parmi $1, \ldots, n$. Encore par l'hypothèse de récurrence, il existe $\binom{n}{k}$ possibilités de choisir k éléments parmi $1, 2, \ldots, n$; c'est-à-dire qu'il existe $\binom{n}{k}$ possibilités de choisir k entiers parmi $1, 2, \ldots, n+1$ à la condition que $n+1$ n'est pas choisi.

Donc, le nombre de possibilités de choisir k entiers parmi $1, 2, \ldots, n+1$ est

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k},$$

par la formule de Pascal (proposition 1.18).

□

Par exemple, le nombre de possibilités de choisir 6 nombres parmi $1, 2, \ldots, 49$ (Lotto allemand) est $\binom{49}{6} = 13983816$.

Théorème 1.20 (Formule du binôme de Newton)**.** *Soit $n \in \mathbb{N}$. Pour tout a, b (nombres réels, rationnels, complexes, entiers, etc.) nous avons :*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Démonstration. Par récurrence.

Initialisation : Pour $n = 0$ on a $(a+b)^0 = 1$ et $\sum_{k=0}^{0} \binom{n}{k} a^k b^{n-k} = \binom{0}{0} a^0 b^0 = 1$, donc l'assertion est vraie.

Hérédité : « $n \Rightarrow n+1$ » : Nous supposons que pour $n \in \mathbb{N}$ l'égalité $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ a déjà été démontrée. Nous faisons le calcul suivant :

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)^n \cdot (a+b) \\
&= \Big(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\Big) \cdot (a+b) \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1} \\
&= \sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n-(k-1)} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1} \\
&= a^0 b^{n+1} + \sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k} \right) a^k b^{n+1-k} + a^{n+1} b^0 \\
&= a^0 b^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^k b^{n+1-k} + a^{n+1} b^0 \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}
\end{aligned}$$

Nous avons utilisé la formule de Pascal (proposition 1.18).

□

2 Logique élémentaire

Objectifs :

- Maîtriser la conjonction, disjonction, négation d'assertions ainsi que les implications, l'équivalence et la contraposée ;
- maîtriser les quantificateurs $\forall$ et $\exists$;
- maîtriser le calcul avec les tables de vérité.

Une grande partie du contenu de cette section a déjà été traitée dans le cours de M. Schlenker pendant la semaine préparatoire. On donnera donc parfois moins de détails au cours.
Dans la section précédente, nous avons déjà considéré le concept des assertions et nous avons introduit d'un point de vue intuitif les implications et l'équivalence. Nous allons maintenant étudier d'autres opérations sur les assertions et formaliser les implications.

Et et ou ou ou et et

Si on a une assertion, son contraire en est une autre, appelée sa **négation** (par ex. « Il pleut. » Négation : « Il ne pleut pas. »). On peut aussi combiner deux assertions par un « **et** » ou un « **ou** » (par ex. « x est pair **et** x est positif. » ; « $x = 2$ **ou** x est impair. »).

Nous allons étudier ces trois constructions de plus près. Pour cela nous allons utiliser les tables de vérité. Pour ceux qui aiment bien l'informatique, cela peut aider d'utiliser le modèle des circuits électriques comme dans le livre de Schichl/Steinbauer.

Définition 2.1. *Soient A et B des assertions.*

(a) **La conjonction « et » (symbole : $\wedge$)**

« Et » en mathématiques a la même signification qu'au quotidien :

L'assertion A et *B (en symboles : $A \wedge B$) est vraie si et seulement si A et B sont vraies.*

(b) **La disjonction « ou » (symbole : $\vee$)**

« Ou » en mathématiques a la signification suivante :

L'assertion « A ou B » (en symboles : $A \vee B$) est vraie si au moins une des assertions A, B est vraie.

(c) **La négation (symbole : $\neg$)**

La négation de A est l'assertion « non A » (en symboles : $\neg A$) qui est vraie si et seulement si A est faux.

Introduisons maintenant le formalisme (facile !) des tables de vérité (v= vrai, f = faux) à l'exemple de la conjonction.

A	B	$A \wedge B$	Explication
v	v	v	Si A est vrai et B est vrai, alors $(A \wedge B)$ est vrai.
v	f	f	Si A est vrai et B est faux, alors $(A \wedge B)$ est faux.
f	v	f	Si A est faux et B est vrai, alors $(A \wedge B)$ est faux.
f	f	f	Si A est faux et B est faux, alors $(A \wedge B)$ est faux.

(1) P est étudiant(e) de ce cours **et** P habite à Luxembourg.
(2) $x^2 = 1$ **et** $x > 0$

Regardons (2) de plus près. Soit A l'assertion « $x^2 = 1$ » et B l'assertion « $x > 0$ ».

- $x = 1$: c'est le cas de la rangée 1 ; alors, l'assertion est vraie.
- $x = -1$: c'est le cas de la rangée 2 ; alors, l'assertion est fausse.
- $x \neq 1$ et $x > 0$: c'est le cas de la rangée 3 ; alors, l'assertion est fausse.
- $x \neq -1$ et $x \leq 0$: c'est le cas de la rangée 4 ; alors, l'assertion est fausse.

Voici, la table de vérité pour la disjonction :

A	B	$A \vee B$
v	v	v
v	f	v
f	v	v
f	f	f

(1) P est étudiant(e) de ce cours **ou** P habite à Luxembourg.
(2) $x^2 = 1$ **ou** $x > 0$

Regardons (2) de plus près. Soit A l'assertion « $x^2 = 1$ » et B l'assertion « $x > 0$ ».

- $x = 1$: c'est le cas de la rangée 1 ; alors, l'assertion est vraie.
- $x = -1$: c'est le cas de la rangée 2 ; alors, l'assertion est vraie.
- $x \neq 1$ et $x > 0$: c'est le cas de la rangée 3 ; alors, l'assertion est vraie.
- $x \neq -1$ et $x \leq 0$: c'est le cas de la rangée 4 ; alors, l'assertion est fausse.

Notez que « ou » au quotidien est souvent utilisé de manière exclusive : « Voulez vous du café ou du thé ? » ; « Allez-vous à droite ou à gauche ? ». C'est soit l'un, soit l'autre. Pas en maths : Si A et B sont vraies, alors l'assertion $(A \vee B)$ est vraie. Mais, aussi au quotidien on peut utiliser « ou » comme en maths : « Si c'est votre anniversaire ou si vous réussissez l'examen, je vous félicite. » Je vous félicite même si vous réussissez votre examen le jour de votre anniversaire.
Pour être comlet, nous donnons la table de vérité de la négation qui est facile.

A	$\neg A$
v	f
f	v

Voici, des exemples de négations :

(1) Il pleut.
Négation : Il ne pleut pas.
(2) $x = 1$
Négation : $x \neq 1$
(3) Il est luxembourgeois **et** il étudie à l'Université du Luxembourg.
Négation : Il n'est pas luxembourgeois **ou** il n'étudie pas à l'Université du Luxembourg.
(4) $x^2 = 1$ **et** $x > 0$
Négation : $x^2 \neq 1$ **ou** $x \leq 0$

Soulignons ce que nous avons vu dans les exemples (3) et (4) :

Lors de la négation, « et » et « ou » sont à échanger !

Voici la proposition qui exprime cela.

Proposition 2.2 (De Morgan)**.** *Soient A, B des assertions. Alors :*

(a) $\neg(A \wedge B) = (\neg A) \vee (\neg B)$,

(b) $\neg(A \vee B) = (\neg A) \wedge (\neg B)$.

Démonstration. L'assertion (a) se voit par l'égalité de la 3ème et la dernière colonne dans la table de vérité :

A	B	$A \wedge B$	$\neg(A \wedge B)$	$\neg A$	$\neg B$	$(\neg A) \vee (\neg B)$
v	v	v	f	f	f	f
v	f	f	v	f	v	v
f	v	f	v	v	f	v
f	f	f	v	v	v	v

La démonstration de (b) est similaire. □

Mentionnons encore la **double négation** : on vérifie immédiatement que $\neg(\neg A) = A$; donc la négation de la négation d'une assertion est égale à l'assertion du début : s'il est faux que l'assertion A est fausse, alors A est vraie. Voici, quelques exemples :

- Il n'est pas vrai que le Luxembourg n'appartient pas à l'UE.
- Je ne vais pas m'abstenir de voter.
- « $\neg(x \neq 1)$ » est une façon compliquée pour écrire « $x = 1$ ».

Pour finir, nous donnons un théorème qui résume quelques règles pour le calcul avec les symboles $\vee, \wedge, \neg$. La démonstration se fait par tables de vérité.

Théorème 2.3. *Soient A, B, C des assertions. Alors les égalités suivantes sont vraies.*

(a) $A \vee B = B \vee A$,
$A \wedge B = B \wedge A$ *(commutativité) ;*

(b) $A \vee (B \vee C) = (A \vee B) \vee C$,
$A \wedge (B \wedge C) = (A \wedge B) \wedge C$ *(associativité) ;*

(c) $A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$,
$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$ *(distributivité) ;*

(d) $A \vee (B \wedge A) = A$,
$A \wedge (B \vee A) = A$ *;*

(e) $A \vee A = A$,
$A \wedge A = A$ *;*

(f) $A \vee f = A$,
$A \wedge v = A$ *; ici, v et f sont les assertions qui sont toujours vraies/fausses.*

(g) $A \vee v = v$,
$A \wedge f = f$ *;*

(h) $A \vee (\neg A) = v$,
$A \wedge (\neg A) = f$ *;*

(i) $\neg(\neg A) = A$ *;*

(j) $\neg(A \vee B) = (\neg A) \wedge (\neg B)$*,*
$\neg(A \wedge B) = (\neg A) \vee (\neg B)$ *(règles de de Morgan).*

De l'existence pour tout

Il y a peut-être une personne parmi vous qui a deux frères. Est-ce que cette personne dit la vérité quand elle dit : « J'ai un frère » ? Evidemment que oui ! Si on a deux frères, on en a aussi un. Un mathématicien ayant un frère et pas deux dirait : « J'ai un frère et un seul » ou « J'ai précisement un frère. »
Une autre personne n'a pas de frère du tout. A-t-elle raison si elle dit : « Tous mes frères ont les cheveux verts » ? La réponse est encore : oui.

« Il existe » veut dire : il existe au moins un. Il peut y en avoir plus d'un. Souvent on utilise le symbole $\exists$ pour « il existe ». S'il existe un, mais pas deux ou plus, alors on dit que « il existe un et un seul » ou « il existe un unique ». Dans ce cas, on écrit souvent « $\exists!$ ». Les deux points « : » possèdent la signification « tel(s) que ». Le symbole $\forall$ signifie « pour tout ».
Exemples :

(1) (vrai) Il y a un étudiant dans cette salle.

(2) (vrai) Il existe un nombre rationnel x tel que $2x = 2$ (en symboles : $\exists\, x \in \mathbb{Q} : 2x = 2$).

(3) (vrai) Il existe un et un seul nombre rationnel x tel que $2x = 2$ (en symboles : $\exists!\, x \in \mathbb{Q} : 2x = 2$).

(4) (vrai) Il existe un nombre rationnel x tel que $x^2 = 1$ (en symboles : $\exists\, x \in \mathbb{Q} : x^2 = 1$).

(5) (vrai) Il existe un et un seul nombre rationnel x tel que $x^2 = 1$ et $x > 0$ (en symboles : $\exists!\, x \in \mathbb{Q} : (x^2 = 1 \wedge x > 0)$).

(6) (faux) Il existe un et un seul nombre rationnel x tel que $x^2 = 1$ (en symboles : $\exists!\, x \in \mathbb{Q} : x^2 = 1$).

(7) (vrai) L'équation $a^2 + b^2 = c^2$ possède une solution en entiers positifs non nuls.
Démonstration. $3^2 + 4^2 = 5^2$.

(8) (vrai) Tous les étudiants dans cette salle étudient à l'Université du Luxembourg.

(9) (vrai) Pour tout nombre rationnel x, on a $x^2 \geq 0$ (en symboles : $\forall\, x \in \mathbb{Q} : x^2 \geq 0$)).

(10) (vrai) Le carré de tout entier relatif pair est divisible par 4 (en symboles : $\forall\, n \in \mathbb{Z} : (2 \mid n \Rightarrow 4 \mid n^2)$).
Démonstration : Soit $n \in \mathbb{Z}$ (arbitraire) tel que $2 \mid n$. Alors, $n = 2m$ pour un $m \in \mathbb{Z}$ et donc $n^2 = 4m^2$ est divisible par 4.

(11) (vrai) Tout nombre réel non-négatif est le carré d'un nombre réel non-négatif (en symboles : $\forall\, x \in \mathbb{R}_{\geq 0}, \exists\, y \in \mathbb{R}_{\geq 0} : y^2 = x$ où $\mathbb{R}_{\geq 0}$ est l'ensemble de tous les nombres réels non-négatifs).
Démonstration : Soit $x \in \mathbb{R}_{\geq 0}$ (arbitraire). On prendra $y = \sqrt{x}$, sa racine carrée.

(12) (faux) Le carré de tout nombre réel est supérieur à 0 (en symboles : $\forall\, x \in \mathbb{Q} : x^2 > 0$).
Démonstration : L'assertion est fausse pour $x = 0$.

Pour démontrer une assertion d'existence, il suffit de donner un exemple. Pour démontrer une assertion de la forme « $\forall\, x \in E : A(x)$ », on se donne un $x \in E$ (arbitraire) et on démontre $A(x)$ pour ce x. Pour démontrer qu'une assertion de la forme « $\forall\, x \in E : A(x)$ » est fausse, il suffit de donner un contre-exemple.

Le dernier point suit en fait du premier par les règles de négation que nous regardons maintenant.

(1) Tous les étudiants ont les cheveux blonds.
Négation : Il existe un étudiant qui n'a pas les cheveux blonds.

(2) Il existe x tel que $f(x) = 0$.
Négation : Pour tout x : $f(x) \neq 0$.

Si on fait la négation d'une assertion, il faut échanger $\forall$ et $\exists$, et il faut échanger « $\wedge$ » et « $\vee$ ».

La table de vérité de l'implication

Nous définissons maintenant l'implication $A \Rightarrow B$ par la table de vérité :

A	B	$A \Rightarrow B$
v	v	v
v	f	f
f	v	v
f	f	v

Voici une explication du choix de cette définition. Supposons que $A \Rightarrow B$ est vraie. Alors :

- Si A est vraie, B est vraie aussi. Ceci exprime « l'implication ».
- Si A est fausse, on ne peut rien dire sur B : B peut être vraie ou fausse.

En fait, si on exige ces deux propriétés, la table de vérité de $A \Rightarrow B$ ne peut être que celle en haut, comme on le vérifie directement. Il peut apparaître contre-intuitif que les dernières deux lignes expriment : « D'une fausse assertion A on peut conclure que toute assertion B est vraie et qu'elle est fausse. »

Proposition 2.4. *Soient A, B des assertions. Alors :*

(a) $(A \Rightarrow B) = ((\neg A) \vee B)$.

(b) $(A \Rightarrow B) = (\neg(A \wedge (\neg B)))$.

(c) $(A \Rightarrow B) = ((\neg A) \Leftarrow (\neg B))$.

La démonstration se fait par une table de vérité.
La partie (b) de la proposition 2.4 donne une explication formelle pour les démonstrations par l'absurde : si l'assertion « l'hypothèse A est vraie et la conclusion B est fausse » est fausse (par exemple, parce qu'on trouve une contradiction), alors $A \Rightarrow B$ est vrai.
Elle justifie aussi (encore une fois) la table de vérité définissant l'implication (« On ne peut pas avoir à la fois A vraie et B fausse »).

La contraposée

Soient A et B deux assertions. On appelle l'assertion « $(\neg A) \Leftarrow (\neg B)$ » la *contraposée de* $(A \Rightarrow B)$. La partie (c) de la proposition 2.4 nous dit que l'assertion « $A \Rightarrow B$ » est vraie, si et seulement si « $(\neg A) \Leftarrow (\neg B)$ » est vraie.

(1) Il pleut. $\Rightarrow$ La rue est mouillée.
Formulation équivalente : Il ne pleut pas. $\Leftarrow$ La rue n'est pas mouillée.

(2) P est un point sur le cercle de rayon r et de centre C. $\Rightarrow$ La distance entre P est C est égale à r.
Formulation équivalente : P n'est pas un point sur le cercle de rayon r et de centre C. $\Leftarrow$ La distance entre P est C est différente de r.

(3) $x = 1 \Rightarrow x^2 = 1$
Formulation équivalente : $x \neq 1 \Leftarrow x^2 \neq 1$

(4) $x^2 = 1$ et $x > 0 \Leftrightarrow x = 1$
Formulation équivalente : ($x^2 \neq 1$ ou $x \leq 0$) $\Leftrightarrow x \neq 1$

Quelquefois il est plus facile de démontrer la contraposée d'une assertion que l'assertion elle-même.

Proposition 2.5. *Si* $x^7 + x + 1 = 0$, *alors* $x \neq 1$.

Démonstration. Nous ne cherchons pas à calculer les solutions de cette équation car elles ne sont pas demandées. Il est plus facile de démontrer la contraposée : « Si $x = 1$ alors $x^7 + x + 1 \neq 0$. » On voit immédiatement que cette assertion est vraie car $1^7 + 1 + 1 = 3 \neq 0$. □

Ne pas confondre la contraposée $(\neg A) \Leftarrow (\neg B)$ avec $(\neg A) \Rightarrow (\neg B)$.

Voici un exemple d'une utilisation erronnée (!) :

> Les voitures ayant eu un accident sont cassées. Cette voiture n'a pas eu d'accident, alors elle n'est pas cassée.

Nous connaissons maintenant les principes les plus importants des démonstrations :

- démonstration directe ;
- démonstration de la contraposée (c'est une démonstration indirecte) ;
- démontration par l'absurde (c'est une démonstration indirecte) ;
- démonstration qu'une assertion est fausse par un contrexemple ;
- démonstration par récurrence.

3 Ensembles

Objectifs :

- Maîtriser la notion intuitive d'ensemble, union, intersection, complément, etc.
- savoir démontrer des propriétés simples.

Cette section provient du cours préparatoire. Elle ne sera traitée que brièvement.

Introduction

Les ensembles sont un outil indispensable en mathématiques. Nous en avons notamment besoin pour décrire des fonctions. Notre approche des ensembles sera celle du 19ème et du début du 20ème siècle. Une théorie plus rigoureuse ne peut pas être enseignée au début des études.

On peut décrire un ensemble en écrivant ses éléments. Par exemple :

- $\mathcal{A} = \{A, B, C, D, \ldots, X, Y, Z\}$, l'alphabet.
- $\mathcal{Z} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, l'ensemble des chiffres.

On utilise les accolades pour indiquer qu'il s'agit d'un ensemble. Les 'objets' dans un ensemble sont appelés *éléments*.
Vous connaissez déjà des ensembles de l'école :

- $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ l'ensemble des nombres naturels/entiers non-négatifs,
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ l'ensemble des entiers relatifs,
- $\mathbb{Q}$, l'ensemble des nombres rationnels (les fractions),
- $\mathbb{R}$, l'ensemble des nombres réels,
- $\mathbb{C}$, l'ensemble des nombres complexes (voir le cours à ce sujet).

Nous utiliserons les notations suivantes :

- $\emptyset$ pour l'ensemble vide ;
- $\in$ pour indiquer l'appartenance d'un élément à un ensemble ;
- $\notin$ pour indiquer qu'un élément n'appartient pas à un ensemble ;
- $\#M$ pour indiquer le nombre d'éléments (le cardinal) d'un ensemble.

Par exemple :

- $7 \in \mathbb{R}$
- $7 \in \mathbb{N}$
- $7 \in \mathbb{Z}$

- $-1 \notin \mathbb{N}$
- $1/2 \in \mathbb{Q}$
- $1/2 \notin \mathbb{Z}$
- $A \in \mathcal{A}$ (A est élément de l'ensemble $\mathcal{A}$, l'alphabet.)
- $A \notin \mathcal{Z}$ (A n'est pas un élément de l'ensemble des chiffres $\mathcal{Z}$.)
- $\#\mathcal{A} = 26$
- $\#\mathcal{Z} = 10$

Nous exigeons que les ensembles satisfassent les deux propriétés fondamentales suivantes :

- Les éléments d'un ensemble sont tous deux-à-deux distincts, c'est-à-dire qu'un seul objet n'est pas deux fois élément d'un seul ensemble : $\{1, 2, 2, 3\}$ n'est qu'une écriture (non-minimale) de $\{1, 2, 3\}$.
- Les éléments d'un ensemble ne sont pas ordonnés, c'est-à-dire qu'un ensemble ne dépend pas de l'ordre dans lequel on écrit ses éléments : $\{1, 2, 3\} = \{2, 3, 1\}$.

Une autre façon d'écrire un ensemble est de le définir par des propriétés de ses éléments. Par exemple :

- $\mathcal{X} = \{ \underbrace{xy}_{\text{éléments}} \mid \underbrace{x \in \mathcal{Z}, y \in \mathcal{Z}}_{\text{propriétés}} \} = \{00, 01, 02, 03, \ldots, 99\}$.
- $\mathcal{E} = \{P \mid P \text{ est étudiant(e) de ce cours }\}$, l'ensemble des étudiants de ce cours.
- $\mathcal{L} = \{P \mid P \text{ est un/une Luxembourgeois(e) }\}$, l'ensemble de tous les Luxembourgeois.
- $\mathcal{B} = \{ABC \mid A \in \mathcal{A}, B \in \mathcal{A}, C \in \mathcal{A}\}$, l'ensemble de tous les mots de trois lettres. Noter que la virgule dans la description doit être comprise comme « et » et pourrait être remplacée par « $\wedge$ ».
- $\mathcal{G} = \{n \mid n \in \mathbb{N}, n \text{ est pair }\}$, l'ensemble des nombres naturels pairs.
- Soient $a, b \in \mathbb{R}$. L'ensemble

$$[a, b] := \{x \mid x \in \mathbb{R}, a \leq x \leq b\}$$

est appelé *l'intervalle fermé entre a et b*. (Pour les intervalles ouverts (semi-ouverts), on utilise la notation $]a, b[$ ($]a, b]$).)

La notion d'ensemble de Georg Cantor

La notion d'ensemble utilisée dans ce cours (et pendant la plupart de vos études) est celle de Georg Cantor :

> Par ensemble, nous entendons toute collection M d'objets m de notre intuition ou de notre pensée, définis et distincts, ces objets étant appelés les éléments de M.

Interprétation :

- objet : « objet mathématique » ;
- collection : l'ensemble sera un nouvel objet mathématique ;
- définis : les objets doivent être clairement définis ;
- distincts : il doit être clair si deux objets sont égaux ou distincts.

Il y a des subtilités avec les ensembles que vous n'allez pas rencontrer pendant vos études (sauf dans un cours de logique mathématique). C'est à cause de cela qu'il faut en fait utiliser une notion plus moderne. Pour les mathématiques que nous allons faire, cela ne fera aucune différence.
Voici un problème avec la notion de Cantor : le paradoxe de Russell. Il en suit qu'il n'existe pas d'ensemble de tous les ensembles.
En effet, supposons par l'absurde que l'ensemble de tous les ensembles existe ; appelons le Ω. Nous pouvons alors considérer le sous-ensemble A de Ω formé des ensembles X tels que X n'est pas un élément de l'ensemble X :

$$A = \{X \in \Omega | X \notin X\}\,.$$

Qu'en est-il alors de A ? Si A est un élément de A ($A \in A$), alors par définition de A, A n'est pas un élément de A ($A \notin A$). Et si A n'est pas un élément de A ($A \notin A$), alors par définition de A, A est un élément de A ($A \in A$). Aucune de ces deux options n'est donc possible.

Sous-ensembles et opérations sur les ensembles

Définition 3.1. *Soient A, B des ensembles.*

- *B est appelé* sous-ensemble/partie de *A si pour tout $b \in B$ on a $b \in A$. Notation : $B \subseteq A$.*
- *A et B sont appelés* égaux *si $A \subseteq B$ et $B \subseteq A$. Notation : $A = B$.*
- *On appelle l'ensemble*
$$A \setminus B := \{a \mid a \in A, a \notin B\}$$
le complément ou la différence de B dans A.
- *On appelle l'ensemble*
$$A \cup B := \{a \mid a \in A \vee a \in B\}$$
la réunion de A et B.

- *On appelle l'ensemble*
$$A \cap B := \{a \mid a \in A \wedge a \in B\}$$
l'intersection de A et B.
- *Si on a* $A \cap B = \emptyset$*, on appelle* $A \cup B$ *la* réunion disjointe de A et B. *Notation :* $A \dot{\cup} B$ *ou* $A \sqcup B$.
- *On appelle l'ensemble*
$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$
le produit cartésien de A et B. *Ses éléments sont aussi appelés* couples.

Par exemple :

- $\{A, D, Z\} \subseteq \mathcal{A}$.
- $\{1, 2, 3, 4\} \subseteq \mathcal{Z}$; aussi : $\{1, 2, 3, 4\} \subseteq \mathbb{N}$.
- $\mathcal{G} \subseteq \mathbb{N}$
- $[1, 2] \subseteq \mathbb{R}$
- $\mathcal{Z} \setminus \{1, 2, 3, 4\} = \{0, 5, 6, 7, 8, 9\}$.
- $\{1, 2, 3, 4\} \setminus \{2, 3, 4, 5\} = \{1\}$.
- $\{1, 2, 3\} \setminus \mathcal{Z} = \emptyset$.
- $[1, 3] \setminus [2, 3] = [1, 2[$.
- $\{1, 2\} \cup \{8, 9\} = \{1, 2, 8, 9\} = \{1, 2\} \dot{\cup} \{8, 9\}$
- $\{1, 2, 3\} \cup \{3, 4, 5\} = \{1, 2, 3, 4, 5\}$. (Tout élément n'appartient qu'une fois à l'ensemble !)
- $[1, 3] \cap [2, 4] = [2, 3]$
- $\mathcal{L} \cap \mathcal{E} = \{A \mid A$ est Luxembourgeois et étudiant de ce cours $\}$.
- $\mathbb{N} \times \mathbb{N}$ est l'ensemble de tous les couples (a, b) avec $a, b \in \mathbb{N}$.
- $\mathcal{A} \times \mathcal{Z} = \{(A, 0), (A, 1), \ldots, (A, 9), (B, 0), (B, 1), \ldots, (B, 9), (C, 0), \ldots, (Z, 9)\}$.
- $\{n \mid n \in \mathbb{Z}, 2$ divise $n\} \cap \{n \mid n \in \mathbb{Z}, 3$ divise $n\} = \{n \mid n \in \mathbb{Z}, 6$ divise $n\}$.

Quelques propriétés

Lemme 3.2. *Soient* A, B, C *des ensembles. Alors, les assertions suivantes sont vraies :*

(a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

(b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Démonstration. (a) Nous nous souvenons que deux ensembles sont égaux si l'un est sous-ensemble de l'autre et réciproquement. Nous allons alors montrer les deux inclusions :

(1) $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$

(2) $A \cap (B \cup C) \supseteq (A \cap B) \cup (A \cap C)$

Par définition de $\subseteq$ il faut montrer :

(1) $x \in A \cap (B \cup C) \Rightarrow x \in (A \cap B) \cup (A \cap C)$.

(2) $x \in (A \cap B) \cup (A \cap C) \Rightarrow x \in A \cap (B \cup C)$.

(1) Soit $x \in A \cap (B \cup C)$.
$\Rightarrow x \in A \wedge x \in (B \cup C)$
$\Rightarrow x \in A \wedge (x \in B \vee x \in C)$
$\Rightarrow (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)$
$\Rightarrow x \in A \cap B \vee x \in A \cap C$
$\Rightarrow x \in (A \cap B) \cup (A \cap C)$
Nous avons démontré (1). Dans les calculs on s'est servi des règles pour le calcul avec les symboles « $\vee$, $\wedge$ » du théorème 2.3.
(2) Soit $x \in (A \cap B) \cup (A \cap C)$
$\Rightarrow x \in A \cap B \vee x \in A \cap C$
$\Rightarrow (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)$
$\Rightarrow x \in A \wedge (x \in B \vee x \in C)$
$\Rightarrow x \in A \cap (B \cup C)$.
Nous avons démontré (2), et donc (a).
(b) Exercice 3.5. □

Nous avons vu que l'intersection correspond au « et/$\wedge$ » et la réunion au « ou/$\vee$ ». Dans le prochain lemme nous voyons que le complément correspond à la négation.

Lemme 3.3. *Soient E un ensemble, A et B des parties de E et $\overline{A} = E \setminus A$ et $\overline{B} = E \setminus B$, les complémentaires de A et B dans E ; on a :*

(a) $A \cap \overline{A} = \emptyset$ *et* $A \cup \overline{A} = E$ *(autrement dit* $A \sqcup \overline{A} = E$*) ;*

(b) $E \setminus (E \setminus A) = A$ *(autrement dit* $\overline{\overline{A}} = A$*) ;*

(c) $A \subseteq B \Leftrightarrow \overline{B} \subseteq \overline{A}$ *;*

(d) $\overline{A \cup B} = \overline{A} \cap \overline{B}$ *;*

(e) $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Démonstration.

(a) Supposons par l'absurde que l'intersection $A \cap \overline{A}$ est non vide. Soit alors x un élément dans $A \cap \overline{A}$. On a : $x \in A \wedge x \notin A$. Ceci est impossible, donc $A \cap \overline{A}$ est vide.

Comme A et $\overline{A}$ sont des sous-ensembles de E, leur union l'est aussi : on a $A \cup \overline{A} \subseteq E$. Démontrons maintenant que E est inclus dans l'union $A \cup \overline{A}$. Pour cela, soit x un élément de E. On a : $x \in A \vee x \notin A$. Ceci prouve que x appartient à $A \cup \overline{A}$. Ainsi, on a $E \subseteq A \cup \overline{A}$, et finalement l'égalité.

(b) Soit x dans E ; on a :

$$x \in E \setminus (E \setminus A) \Leftrightarrow x \notin E \setminus A \Leftrightarrow \neg(x \in E \setminus A) \Leftrightarrow \neg(x \notin A) \Leftrightarrow x \in A.$$

Ceci prouve l'égalité des deux ensembles.

(c) La clé dans cette démonstration est la contraposée. Par définition, l'inclusion $\overline{B} \subseteq \overline{A}$ signifie

$$\forall\, x \in E : (x \notin B \Rightarrow x \notin A).$$

On reconnaît que l'assertion entre paranthèses est la contraposée de l'assertion entre paranthèses de

$$\forall\, x \in E : (x \in A \Rightarrow x \in B),$$

qui signifie précisement $A \subseteq B$.

(d) Soit x dans E ; on a :

$$x \in \overline{A \cup B} \Leftrightarrow x \notin A \cup B \Leftrightarrow \neg(x \in A \cup B) \Leftrightarrow \neg(x \in A \vee x \in B)$$

$$\Leftrightarrow \neg(x \in A) \wedge \neg(x \in B) \Leftrightarrow x \in \overline{A} \wedge x \in \overline{B} \Leftrightarrow x \in \overline{A} \cap \overline{B}.$$

Ceci prouve l'égalité des deux ensembles.

(e) On a, d'après (b) et (d) :

$$\overline{A \cap B} = \overline{\overline{\overline{A}} \cap \overline{\overline{B}}} = \overline{\overline{\overline{A} \cup \overline{B}}} = \overline{A} \cup \overline{B}.$$

□

Exercices sur les ensembles

Exercice 3.4. *Soient*

$$A = \{n \mid n \in \mathbb{N}, n \text{ est divisible par } 2\} \text{ et } B = \{n \mid n \in \mathbb{N}, n \text{ est divisible par } 5\}.$$

(a) Décrire l'intersection $A \cap B$.

(b) Décrire la réunion $A \cup B$.

(c) Décrire le complément $B \setminus A$.

(d) Décrire le complément $A \setminus B$.

(e) Donner le cardinal de $[12, 27] \cap A$ *et de* $[12, 27] \cap B$.

Exercice 3.5. *(Deuxième partie du lemme 3.2.) Soient* A, B *et* C *des ensembles. Démontrer :*

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Exercice 3.6. *(a) Soient* A *et* B *des ensembles. Démontrer :*

(1) $A \subseteq B \iff A = A \cap B \iff B = A \cup B$ *;*
(2) $A \cap B = \emptyset \iff A \setminus B = A$.

(b) Soient E *un ensemble et* A, B *des sous-ensembles de* E. *Démontrer :*

(1) $A \cap B = \emptyset \iff B \subseteq E \setminus A \iff A \subseteq E \setminus B$ *;*
(2) $A \cup B = E \iff E \setminus A \subseteq B \iff E \setminus B \subseteq A$.

Corrigé des exercices sur les ensembles

Exercice 3.4. Soient

$$A = \{n \mid n \in \mathbb{N}, n \text{ est divisible par } 2\} \text{ et } B = \{n \mid n \in \mathbb{N}, n \text{ est divisible par } 5\}.$$

(a) $A \cap B = \{n \mid n \in \mathbb{N}, n$ est divisible par $10\}$.

Raison : un entier relatif n est divisible par 10 si et seulement s'il est divisible par 2 et 5.

(b) $A \cup B = \{n \mid n \in \mathbb{N}, n$ est divisible par 5 ou par $2\}$.

(c) $B \setminus A = \{n \mid n \in \mathbb{N}, n$ est divisible par 5 et n'est pas divisible par $10\}$.

(d) $A \setminus B = \{n \mid n \in \mathbb{N}, n$ est divisible par 2 et n'est pas divisible par $5\}$.

(e) $[12, 27] \cap A = \{12, 14, 16, 18, 20, 22, 24, 26\}$, donc son cardinal est 8.
$[12, 27] \cap B = \{15, 20, 25\}$, donc son cardinal est 3.

Exercice 3.5. Soient A, B et C des ensembles. On a :

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Avec la même argumentation que pour (a) du lemme 3.2, nous devons démontrer :

(1) $x \in A \cup (B \cap C) \Rightarrow x \in (A \cup B) \cap (A \cup C)$.

(2) $x \in (A \cup B) \cap (A \cup C) \Rightarrow x \in A \cup (B \cap C)$.

(1) Soit $x \in A \cup (B \cap C)$
$\Rightarrow x \in A \vee x \in (B \cap C)$
$\Rightarrow x \in A \vee (x \in B \wedge x \in C)$
$\Rightarrow (x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$
$\Rightarrow x \in A \cup B \wedge x \in A \cup C$

$\Rightarrow x \in (A \cup B) \cap (A \cup C)$
Nous avons démontré (1).
(2) Soit $x \in (A \cup B) \cap (A \cup C)$
$\Rightarrow x \in A \cup B \wedge x \in A \cup C$
$\Rightarrow (x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$
$\Rightarrow x \in A \vee (x \in B \wedge x \in C)$
$\Rightarrow x \in A \vee x \in (B \cap C)$
$\Rightarrow x \in A \cup (B \cap C)$
Nous avons démontré (2) et donc l'assertion demandée.
Exercice 3.6.

(a) Soient A et B des ensembles. On a :

(1) $A \subseteq B \iff A = A \cap B \iff B = A \cup B$.
Raison : Il y a plusieures manières pour démontrer cela. Nous en donnons une.
Commençons par les équivalences suivantes :

$$A \subseteq B \Leftrightarrow (x \in A \Rightarrow x \in B) \Leftrightarrow (x \in A \Leftrightarrow (x \in A \wedge x \in B)) \Leftrightarrow A = A \cap B.$$

Regardons maintenant les équivalences suivantes :

$$A \subseteq B \Leftrightarrow (x \in A \Rightarrow x \in B) \Leftrightarrow (x \in B \Leftrightarrow (x \in A \vee x \in B)) \Leftrightarrow B = A \cup B.$$

(2) $A \cap B = \emptyset \iff A \setminus B = A$.
Raison :

$$A \cap B = \emptyset \Leftrightarrow (x \in A \Rightarrow x \notin B) \Leftrightarrow A \setminus B = \{x \mid x \in A \wedge x \notin B\} = \{x \mid x \in A\} = A.$$

(b) Soient E un ensemble et A, B des sous-ensembles de E. On a :

(1) $A \cap B = \emptyset \Longleftrightarrow B \subseteq E \setminus A \Longleftrightarrow A \subseteq E \setminus B$.
Raison : D'abord nous avons les équivalences

$$A \cap B = \emptyset \Leftrightarrow \forall\, x \in E : (x \in A \Rightarrow x \notin B) \Leftrightarrow A \subseteq E \setminus B.$$

Pour voir le reste il suffit de prendre la contraposée de l'assertion $\forall\, x \in E : (x \in A \Rightarrow x \notin B)$ est $\forall\, x \in E : (x \in B \Rightarrow x \notin A)$ qui équivaut à l'inclusion $B \subseteq E \setminus A$.

(2) $A \cup B = E \Longleftrightarrow E \setminus A \subseteq B \Longleftrightarrow E \setminus B \subseteq A$.
Ces équivalences peuvent être démontrées avec des arguments similaires. Mais il est aussi possible d'appliquer les règles pour les compléments dans le lemme 3.3 à l'assertion (1).

4 Applications et fonctions

Objectifs :

- Maîtriser les notions d'application, d'image, d'image réciproque, etc. ;

- maîtriser les notions d'injectivité, de surjectivité et de bijectivité ;
- savoir démontrer des propriétés simples.

Cette section provient du cours préparatoire. Elle ne sera traitée que brièvement.
Dans ce cours, nous utilisons les mots « application » et « fonction » comme des synonymes.

La notion d'une application/fonction

Commençons par des exemples :

- Considérons l'application $f : \underbrace{\mathbb{R}}_{\text{source}} \to \underbrace{\mathbb{R}}_{\text{but}}$ donnée par la règle $f(x) = x^2$ pour tout $x \in \mathbb{R}$.

  On dit que x^2 est l'image de x par f. Par exemple : 4 est l'image de 2 par f.

  On dit aussi que 2 est une image réciproque/un antécédant de 4 par f. Noter que -2 est un autre antécédant, donc les antécédants ne sont pas uniques.

  Si une application est donnée par une règle comme f, on écrit la règle aussi comme $x \overset{f}{\mapsto} x^2$ ou $x \mapsto x^2$ tout court.

  L'image de f est la partie du but dans laquelle tout élément possède au moins un antécédant. Dans notre cas on a $\mathrm{Im}(f) = \{x \mid x \in \mathbb{R}, x \geq 0\} = \mathbb{R}_{\geq 0}$.

- $A = \{1, 2, 3\}$, $B = \{X, Y\}$. On voudrait définir une application $g : \underbrace{A}_{\text{source}} \to \underbrace{B}_{\text{but}}$. Nous pouvons simplement le faire en posant $g(1) = X$, $g(2) = Y$, $g(3) = X$.

  Une autre possibilité serait $g(1) = X$, $g(2) = Y$, $g(3) = Y$, et encore une autre $g(1) = Y$, $g(2) = Y$, $g(3) = Y$ (c'est une fonction constante).

  Par contre, il n'est ni permis de poser $g(1) = X$, $g(1) = Y$, $g(2) = X$, $g(3) = Y$, ni suffisant de poser $g(1) = X$ et $g(2) = Y$ car :

Dans la définition d'une application/fonction, tout élément de la source doit posséder une et une unique image dans le but.

- On peut définir l'application $S : \mathcal{L} \to \{\text{homme, femme}\}$ par la règle $S(P) =$ homme si la personne P de l'ensemble $\mathcal{L}$ de tous les Luxembourgeois est un homme, et $S(P) =$ femme sinon.

Nous allons formaliser cette notion maintenant.

Définition 4.1. *Soient A, B des ensembles. Une* application $f : A \to B$ *est une règle qui associe à tout élément $a \in A$ un unique élément $f(a) \in B$.*
On appelle A l'ensemble de départ ou la source de f *et B* l'ensemble d'arrivée ou but de f.
Les applications sont aussi appelées fonctions.
Soit $f : A \to B$ une application.

- *Si $a \in A$, on appelle $f(a)$* l'image de a par f.

- *Soit $S \subseteq A$ un sous-ensemble. L'ensemble*

$$f(S) = \{f(s) \mid s \in S\} \subseteq B$$

est appelé l'image (directe) de S par f.

L'ensemble $f(A) = \mathrm{Im}(f)$ est appelé l'image de f *(tout court).*

- *Soit $b \in B$. Tout $a \in A$ tel que $f(a) = b$ est appelé* une image réciproque (ou préimage ou antécédant) de b *(Un tel élément n'existe pas toujours et lorsqu'il existe, il n'est pas unique en général !).*

- *Soit $T \subseteq B$ un sous-ensemble. L'ensemble*

$$f^{-1}(T) = \{a \mid a \in A, f(a) \in T\} \subseteq A$$

est appelé l'image réciproque (ou préimage ou antécédant) de T par f.

- *On appelle l'ensemble*

$$\{(a, f(a)) \mid a \in A\} \subseteq A \times B$$

le graphe de f.

Le graphe de f est comme vous le connaissez (le dessiner).

Injectivité, surjectivité, bijectivité

Définition 4.2. *Soient A, B des ensembles et $f : A \to B$ une application.*

- *L'application f est appelée* injective *si pour tout $x, y \in A$ l'assertion*

$$f(x) = f(y) \Rightarrow x = y$$

est vraie. Noter la formulation équivalente : f est injectif si et seulement si pour tout $x, y \in A$ distincts $x \neq y$ leurs images sont aussi distinctes $f(x) \neq f(y)$.

- *L'application f est appelée* surjective *si pour tout $b \in B$ il existe $a \in A$ tel que $f(a) = b$. Noter que f est surjectif si et seulement si $f(A) = B$.*

- *L'application f est appelée* bijective *si elle est injective et surjective.*

Regardons ce que ces notions veulent dire dans des exemples.

- Considérons encore l'application $f : \mathbb{R} \to \mathbb{R}$ donnée par $x \mapsto x^2$.

  Alors, f n'est pas surjective car, par exemple, -1 ne possède pas d'antécédant. Elle n'est pas injective non plus, puisque $f(-1) = 1 = f(1)$.

- Faisons une petite modification et considérons l'application

$$\begin{array}{rccc} f_1 : & \mathbb{R} & \to & \mathbb{R}_{\geq 0} \\ & x & \mapsto & x^2. \end{array}$$

  Elle est surjective mais pas injective.

- Modifions-la encore un peu et considérons l'application

$$\begin{array}{rccc} f_2: & \mathbb{R}_{\geq 0} & \to & \mathbb{R} \\ & x & \mapsto & x^2. \end{array}$$

  Maintenant, ell est injective mais pas surjective.

- Finalement, considérons l'application

$$\begin{array}{rccc} f_3: & \mathbb{R}_{\geq 0} & \to & \mathbb{R}_{\geq 0} \\ & x & \mapsto & x^2. \end{array}$$

  Maintenant elle est injective et surjective, donc bijective.

- Regardons maintenant le deuxième exemple du début avec $A = \{1, 2, 3\}$, $B = \{X, Y\}$ et l'application $g : A \to B$ par $g(1) = X$, $g(2) = Y$, $g(3) = X$.

  Cette application est surjective. Il suffit qu'il existe une image réciproque pour chaque élément de l'ensemble d'arrivée. Vérifions ceci : une image réciproque de X est 1 (une autre est 3) et une image réciproque de Y est 2.

  Elle n'est pas injective, car 1 et 3 sont deux éléments distincts de A qui ont la même valeur $g(1) = X = g(3)$.

- L'application S est surjective : il existe au moins un Luxembourgeois et au moins une Luxembourgeoise (probablement présentes dans cette salle). Elle n'est pas injective : il y a plus qu'une Luxembourgeoise ou il y a plus qu'un Luxembourgeois (probablement aussi présents dans cette salle).

- Considérons l'application $f : \mathbb{Z} \to \mathbb{Z}$ donnée par la règle $f(n) = 2n$ pour tout $n \in \mathbb{Z}$.

  Son image $f(\mathbb{Z})$ est l'ensemble de tous les entiers relatifs pairs. Alors, elle n'est pas surjective. Mais f est injective : si $f(n) = 2n$ et $f(m) = 2m$ sont égaux, alors, $n = m$.

- Considérons l'application $f : \mathbb{Z} \to \{n \mid n \in \mathbb{Z}, n \text{ est pair }\}$ donnée par la règle $f(n) = 2n$ pour tout $n \in \mathbb{Z}$.

  Elle est bijective.

- Pour tout ensemble A on considère l'application *identité* $\mathrm{id}_A : A \to A$ donnée par la règle $\mathrm{id}_A(a) = a$ pour tout $a \in A$.

  Elle est bijective.

Pour des ensembles finis (c'est-à-dire, de cardinal fini), la proposition suivante est parfois très utile :

Proposition 4.3. *Soient A, B deux ensembles et $f : A \to B$ une application.*

(a) Supposons que A soit fini de cardinal n. Alors, les assertions suivantes sont équivalentes :

(i) f est injectif.

(ii) $\#\mathrm{Im}(f) = \#A = n$.

(b) Supposons que B soit fini de cardinal n. Alors, les assertions suivantes sont équivalentes :

(i) f *est surjectif.*

(ii) $\#\mathrm{Im}(f) = \#B = n$.

(c) Supposons que A, B soient finis de même cardinal n. Alors, les assertions suivantes sont équivalentes :

(i) f *est injectif.*

(ii) f *est surjectif.*

(iii) f *est bijectif.*

Démonstration. (a) $(i) \Rightarrow (ii)$: Comme les images $f(a)$ pour $a \in A$ sont distinctes, il en suit directement que l'image est de cardinal égal à $\#A$.
$(ii) \Rightarrow (i)$: Comme on suppose qu'il existe autant d'images qu'éléments dans la source, les images $f(a)$ pour $a \in A$ sont deux-à-deux dinstinctes, donc f est injectif.
(b) $(i) \Rightarrow (ii)$: Si f est surjectif, alors $\mathrm{Im}(f) = B$, donc en particulier $\#\mathrm{Im}(f) = \#B$.
$(ii) \Rightarrow (i)$: Comme $\mathrm{Im}(f)$ est un sous-ensemble de B, l'hypothèse $\#\mathrm{Im}(f) = \#B$ implique l'égalité $\mathrm{Im}(f) = B$, donc la surjectivité de f.
(c) C'est une conséquence directe de (a) et (b). □

Composition d'applications et application inverse

Définition 4.4. *Soient A, B, C des ensembles et $f : A \to B$ et $g : B \to C$ des applications. On appelle l'application*

$$g \circ f : A \to C, \quad a \mapsto g(f(a))$$

la composée de g et f.

Voici, des exemples :

- Considérons les applications $[1, 2] \xrightarrow{f} [2, 3] \xrightarrow{g} [4, 9]$ données par les règles $f(x) = x + 1$ et $g(x) = x^2$. Alors, l'application $g \circ f$ est donnée par la règle $(g \circ f)(x) = g(f(x)) = g(x+1) = (x + 1)^2$.
- Soit $f : A \to B$ une application. Alors $\mathrm{id}_B \circ f = f$, puisque pour tout $a \in A$ on a $(\mathrm{id}_B \circ f)(a) = \mathrm{id}_B(f(a)) = f(a)$. De la même manière on voit $f \circ \mathrm{id}_A = f$.

Lemme 4.5 (Associativité de la composition d'applications)**.** *Soient A, B, C, D des ensembles et $f : A \to B$, $g : B \to C$ et $h : C \to D$ des applications. Alors, on a $h \circ (g \circ f) = (h \circ g) \circ f$.*

Démonstration. Deux applications $A \to D$ sont égales si elles prennent la même valeur pour chaque $a \in A$. Nous allons vérifier que ceci est le cas pour $h \circ (g \circ f)$ et $(h \circ g) \circ f$. Soit $a \in A$. Nous avons

$$(h \circ (g \circ f))(a) = h\big((g \circ f)(a)\big) = h\big(g(f(a))\big)$$

et

$$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h\big(g(f(a))\big).$$

Puisque les deux expressions sont les mêmes pour tout $a \in A$, nous avons achevé la démonstration. □

Lemme 4.6. *Si $f : A \to B$ est une application bijective, alors il existe une unique application $g : B \to A$ telle que $g \circ f = \mathrm{id}_A$ et $f \circ g = \mathrm{id}_B$. Elle est donnée par la règle $g(b) = a$ où pour tout $b \in B$ on prend l'unique $a \in A$ tel que $f(a) = b$. L'application g est appelée* l'inverse de *f et souvent notée f^{-1} (attention : ne pas confondre la fonction inverse avec l'image réciproque !).*

Démonstration. Il y a deux choses à faire : (1) montrer l'existence d'une telle fonction g et (2) vérifier son unicité.
(1) Existence : Nous avons l'assertion

$$\forall\, b \in B, \exists!\, a \in A : f(a) = b.$$

En effet, l'existence provient de la surjectivité et l'unicité de l'injectivité. On pose $g(b) := a$. On a donc

$$\forall\, b \in B : f(g(b)) = f(a) = b \quad \Rightarrow \quad f \circ g = \mathrm{id}_B.$$

Soit $a \in A$. Pour $b := f(a)$ il existe un unique $a' \in A$ tel que $f(a') = b = f(a)$, donc $a = a'$ par l'injectivité de f. En conséquence, $g(f(a)) = a' = a$ et donc $g \circ f = \mathrm{id}_A$.
(2) Unicité : Supposons que $h : B \to A$ est une application qui satisfait aussi $h \circ f = \mathrm{id}_A$ et $f \circ h = \mathrm{id}_B$.
A cause de $f \circ h = \mathrm{id}_B$ et $f \circ g = \mathrm{id}_B$, nous concluons

$$f \circ h = f \circ g.$$

En conséquence, on a

$$g \circ (f \circ h) = g \circ (f \circ g).$$

L'associativité d'applications (lemme 4.5) implique :

$$(g \circ f) \circ h = (g \circ f) \circ g.$$

On utilisant $g \circ f = \mathrm{id}_A$ nous obtenons :

$$\mathrm{id}_A \circ h = \mathrm{id}_A \circ g.$$

Les égalités $\mathrm{id}_A \circ h = h$ et $\mathrm{id}_A \circ g = g$ impliquent

$$h = g,$$

et la démonstration est complète. □

Exercices sur les fonctions

Exercice 4.7. *Soient $A = \{1, 2, 3, 4, 5\}$ et $B = \{A, B, C, D\}$.*

(a) Décrire une application surjective de A dans B.

(b) Décrire une application de A dans B qui n'est ni surjective ni injective.

(c) Existe-t-il une application injective de A dans B ? Raison ?

(d) Décrire une application injective de B dans A.

(e) Décrire une application de B dans A qui n'est ni surjective ni injective.

(f) Existe-t-il une application surjective de B dans A ? Raison ?

Exercice 4.8. *(a) Trouver une application injective et non bijective de $\mathbb{N}$ dans $\mathbb{N}$.*

(b) Trouver une application surjective et non bijective de $\mathbb{N}$ dans $\mathbb{N}$.

(c) Trouver une bijection entre $\mathbb{N} \times \mathbb{N}$ et $\mathbb{N}$.

Exercice 4.9. *Soit $\sin : \mathbb{R} \to [-1, 1]$ la fonction sinus (connue de l'école) :*

(a) Est-ce que $\sin$ est bijectif ?

(b) Décrire l'image réciproque $\sin^{-1}(\{0\})$.

(c) Décrire l'image réciproque $\sin^{-1}(\{1\})$.

Exercice 4.10. *Soient A, B, C des ensembles et $f : A \to B$ et $g : B \to C$ des applications. Démontrer les assertions suivantes :*

(a) $g \circ f$ est injectif $\Rightarrow$ f est injectif.

(b) Si f et g sont tous les deux injectifs (respectivement surjectifs, respectivement bijectifs), alors $g \circ f$ est injectif (respectivement surjectif, respectivement bijectif).

Corrigé des exercices sur les fonctions

Exercice 4.7. Soient $A = \{1, 2, 3, 4, 5\}$ et $B = \{A, B, C, D\}$.

(a) Décrire une application surjective $f : A \to B$.

Par exemple : $f(1) = A$, $f(2) = B$, $f(3) = C$, $f(4) = D$, $f(5) = A$.

(b) Décrire une application de A dans B qui n'est ni surjective ni injective.

Par exemple : $f(1) = A$, $f(2) = A$, $f(3) = A$, $f(4) = A$, $f(5) = A$.

(c) Existe-t-il une application injective de A dans B ?

Non, car si une telle application injective f existait, nous aurions $\#\mathrm{Im}(f) = \#A = 5$ et $\mathrm{Im}(f) \subseteq B$, mais, B ne possède pas de sous-ensemble de cardinal 5 car $\#B = 4$, contradiction.

(d) Décrire une application injective $g : B \to A$.

Par exemple : $g(A) = 1$, $g(B) = 2$, $g(C) = 3$, $g(D) = 4$.

(e) Décrire une application de B dans A qui n'est ni surjective ni injective.

Par exemple : $g(A) = 1$, $g(B) = 1$, $g(C) = 1$, $g(D) = 1$.

(f) Existe-t-il une application surjective de B dans A ?

Non, car si $g : B \to A$ était surjective, alors on aurait $4 = \#B \geq \#A = 5$, contradiction.

Exercice 4.8.

(a) Trouver une application injective et non bijective de $\mathbb{N}$ dans $\mathbb{N}$.

Par exemple, $f : \mathbb{N} \to \mathbb{N}$, $n \mapsto 2n$.

(b) Trouver une application surjective et non bijective de $\mathbb{N}$ dans $\mathbb{N}$.

Par exemple, $f : \mathbb{N} \to \mathbb{N}$, $n \mapsto \begin{cases} \frac{n}{2} & \text{si } n \text{ est pair,} \\ 0 & \text{si } n \text{ est impair.} \end{cases}$

(c) Trouver une bijection entre $\mathbb{N} \times \mathbb{N}$ et $\mathbb{N}$.

Par exemple :

$$f(n) := \begin{cases} (n - m^2, m) & \text{si } m^2 \leq n \leq m^2 + m \text{ pour un } m \in \mathbb{N}, \\ (m, m^2 + 2m - n) & \text{si } m^2 + m + 1 \leq n \leq (m+1)^2 - 1 \text{ pour un } m \in \mathbb{N}. \end{cases}$$

On comprend cette application au mieux si on fait un petit dessin.

Exercice 4.9. Soit $\sin : \mathbb{R} \to [-1, 1]$ la fonction sinus (connue de l'école) :

(a) Est-ce que $\sin$ est bijectif ?

Non, car $\sin$ n'est pas injectif : par exemple $\sin(0) = \sin(\pi)$.

(b) Décrire l'image réciproque $\sin^{-1}(\{0\})$.

On a $\sin^{-1}(\{0\}) = \{n \cdot \pi \mid n \in \mathbb{Z}\}$.

(c) Décrire l'image réciproque $\sin^{-1}(\{1\})$.

On a $\sin^{-1}(\{1\}) = \{\frac{\pi}{2} + n \cdot 2\pi \mid n \in \mathbb{Z}\}$.

Exercice 4.10. Soient A, B, C des ensembles et $f : A \to B$ et $g : B \to C$ des applications. Démontrer les assertions suivantes :

(a) $g \circ f$ est injectif $\Rightarrow f$ est injectif.

Démonstration (de l'assertion contraposée). Supposons que f n'est pas injectif. Il existe donc $a_1, a_2 \in A$ tels que $a_1 \neq a_2$ et $f(a_1) = f(a_2)$. En conséquence, $g(f(a_1)) = g(f(a_2))$; cela montre que $g \circ f$ n'est pas injectif.

(b) Si f et g sont tous les deux injectifs (respectivement surjectifs, respectivement bijectifs), alors $g \circ f$ est injectif (respectivement surjectif, respectivement bijectif).

Démonstration. Supposons d'abord f, g injectifs et donnons-nous $a_1, a_2 \in A$ tels que $g(f(a_1)) = g(f(a_2))$. L'injectivité de g implique $f(a_1) = f(a_2)$. L'injectivité de f nous donne maintenant $a_1 = a_2$, montrant l'injectivité de $g \circ f$.

Supposons maintenant f, g surjectifs et donnons-nous $c \in C$. La surjectivité de g montre l'existence d'un $b \in B$ tel que $g(b) = c$. Maintenant la surjectivité de f implique l'existence de $a \in A$ tel que $f(a) = b$. Nous avons donc $g(f(a)) = g(b) = c$. Alors $g \circ f$ est surjectif.

Supposons finalement f, g bijectifs. Cela implique que f, g sont injectifs et surjectifs. Par ce que nous venons de voir, $g \circ f$ est injectif et surjectif, donc bijectif.

5 Relations binaires

Objectifs :

- Maîtriser la notion de relation binaire ;
- connaître et savoir démontrer des exemples de relations binaires.

On parle maintenant des relations à deux.
L'égalité dans $\mathbb{Q}$ définit un sous-ensemble de $\mathbb{Q} \times \mathbb{Q}$ comme suit :

$$\{(x, y) \in \mathbb{Q} \times \mathbb{Q} \mid x = y\} \subseteq \mathbb{Q} \times \mathbb{Q}.$$

Si on appelle cet ensemble S, alors, on a l'équivalence pour tout pair $x, y \in \mathbb{Q}$:

$$x = y \quad \Leftrightarrow \quad (x, y) \in S.$$

De la même manière, « $\leq$ » définit aussi un sous-ensemble de $\mathbb{Q}$:

$$\{(x, y) \in \mathbb{Q} \times \mathbb{Q} \mid x \leq y\} \subseteq \mathbb{Q} \times \mathbb{Q}.$$

L'égalité et le « plus petit ou égal à » sont des exemples de relations binaires (le mot « binaire » indique qu'il s'agit d'une relation entre deux objets). Nous allons maintenant formaliser cela.

Définition 5.1. *Soit E un ensemble ; on appelle* relation binaire sur E *toute partie R de l'ensemble $E \times E$.*

Vocabulaire 5.2. *Soient E un ensemble et R une relation binaire sur E. Pour un couple (x, y) de $E \times E$ tel que (x, y) appartient à R, on dit que x* et *y* sont en relation *et on note xRy ou $x \sim_R y$ (ou même $x \sim y$ si R est clair).*

Définitions 5.3. *Une relation binaire R sur un ensemble E est dite :*

- réflexive *si pour tout x dans E on a xRx ;*
- symétrique *si pour tout (x, y) dans $E \times E$ on a $(xRy \Rightarrow yRx)$;*

- antisymétrique *si pour tout* (x, y) *dans* $E \times E$ *on a* $((xRy \text{ et } yRx) \Rightarrow x = y)$ *;*
- transitive *si pour tout* (x, y, z) *dans* $E \times E \times E$ *on a* $((xRy \text{ et } yRz) \Rightarrow xRz)$ *;*
- totale *si pour tout* (x, y) *dans* $E \times E$ *on a* $(xRy \text{ ou } yRx)$.

Exemples 5.4.

(a) L'égalité sur un ensemble E est une relation réflexive, symétrique, antisymétrique, transitive ; elle est non totale dès que E a au moins 2 éléments.

(b) Soient E un ensemble et $\mathcal{P}(E)$ l'ensemble de ses sous-ensembles (appelés aussi parties*). La relation binaire R définie sur $\mathcal{P}(E)$ par $(ARB \Leftrightarrow A \subseteq B)$ est réflexive, transitive, antisymétrique ; elle est non symétrique dès que E est non vide et non totale dès que E a au moins 2 éléments.*

Nous allons rencontrer deux types de relations binaires : les relations d'ordre et les relations d'équivalence. Nous allons commencer par les premières.

Relations d'ordre

Définition 5.5. *Soit E un ensemble ; on appelle* relation d'ordre sur E *une relation binaire sur E qui est réflexive, transitive et antisymétrique.*

Exemples 5.6.

(a) L'égalité est une relation d'ordre.

(b) Sur l'ensemble des parties d'un ensemble, l'inclusion est une relation d'ordre (en générale non totale).

(c) Le « plus petit ou égal à $\leq$ » sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ est une relation d'ordre (totale).

Soient E un ensemble non vide et $\leq$ une relation d'ordre sur E.

Définition 5.7.

- *Un élément a de E est appelé* plus grand élément de E *s'il vérifie :* $\forall x \in E, x \leq a$.
- *Un élément a de E est appelé* plus petit élément de E *s'il vérifie :* $\forall x \in E, a \leq x$.

Remarque 5.8. *Le plus grand et plus petit élément d'un ensemble ordonné n'existent pas toujours, mais lorsqu'ils existent, ils sont uniques.*
Par exemple, 0 est le plus petit élément de $\mathbb{N}$. L'ensemble des entiers relatifs $\mathbb{Z}$ ne possède aucun plus petit élément.

Définition 5.9. *Soit A une partie de E.*

- *Un élément M de E qui vérifie :* $\forall x \in A, x \leq M$ *est appelé* un majorant de A.
- *Un élément m de E qui vérifie :* $\forall x \in A, m \leq x$ *est appelé* un minorant de A.

Par exemple, pour les intervals réels $[a, b]$, $(a, b]$, $[a, b)$ et (a, b), le nombre réel a est un minorant et b est un majorant.

Vocabulaire 5.10. *Une partie qui possède un majorant (respectivement un minorant) est dite* majorée *(respectivement* minorée*).*

Relations d'équivalence

Définition et premiers exemples

Définition 5.11. *Soit E un ensemble ; on appelle* relation d'équivalence sur E *une relation binaire sur E qui est réflexive, symétrique et transitive.*

Exemples 5.12.

(a) L'égalité sur un ensemble est une relation d'équivalence.

(b) Soit E l'ensemble de tous les étudiants à l'UL. Pour $x, y \in E$ on définit $x \sim y$ si les étudiants x et y étudient dans le même programme. [On suppose ici qu'un étudiant n'étudie que dans un seul programme.]

(c) Soit E l'ensemble de tous les étudiants de ce cours. Pour $x, y \in E$ on définit $x \sim y$ si les étudiants x et y ont le même sexe.

(d) Sur l'ensemble des droites affines du plan, le parallélisme est une relation d'équivalence.

(e) Soient E et F des ensembles et f une application de E dans F. La relation binaire R_f définie sur E par

$$\forall (x, y) \in E^2, (xR_f y \Leftrightarrow f(x) = f(y))$$

est une relation d'équivalence. On l'appelle relation d'équivalence associée à f.

Par exemple, si $f : \mathbb{R} \to \mathbb{R}$ est donné par la règle $f(x) = x^2$, alors

$$x \; R_f \; y \Leftrightarrow x^2 = y^2 \Leftrightarrow x = y \vee x = -y.$$

(f) Soit $n \in \mathbb{Z}$. La congruence modulo n (voir exercices) est une relation d'équivalence :

$$x \equiv y \mod n \Leftrightarrow n \mid (x - y).$$

Classes d'équivalence et ensemble quotient

Soient E un ensemble (non-vide) et R une relation d'équivalence sur E fixés.

Définition 5.13. *(a) Soit x dans E ; on appelle* classe d'équivalence de x (pour la relation R) *le sous-ensemble $\{y \in E \mid xRy\}$ de E ; on le note $\bar{x}$.*

(b) Soit ω une classe d'équivalence de E ; tout élément x dans ω est appelé un représentant *de ω.*

(c) L'ensemble des classes d'équivalence de E pour la relation R est appelé ensemble quotient de E par R *; on le note E/R.*

Remarque 5.14. *Les éléments de l'ensemble E/R sont des classes d'équivalences ; ce sont donc eux-mêmes des ensembles (plus précisément, des sous-ensembles de E) !*

Exemples 5.15. *(a) Pour l'égalité sur un ensemble E, on a : $\bar{x} = \{x\}$.*

(b) Pour la relation d'avoir le même sexe pour les étudiants de ce cours, il n'existe que deux classes d'équivalences : celle des hommes et celles des femmes. Chaque homme dans ce cours est un représentant de la classe d'équivalence des hommes.

(c) Chaque étudiant de ce cours est un représentant de la classe d'équivalence « BASI filière mathématiques » pour la relation d'étudier dans le même programme.

(d) Soient E et F des ensembles et f une application de E dans F. Pour la relation d'équivalence R_f, la classe d'un élément x de E est :

$$\bar{x} = \{y \in E \mid f(y) = f(x)\} = f^{-1}(\{f(x)\}).$$

C'est « l'image réciproque de l'image de x ».

Proposition 5.16. *(a) Les classes d'équivalence de E sont toutes non vides et tout élément de E appartient à une et une seule classe d'équivalence (la sienne !).*

(b) Soient $x, y \in E$. Alors :

$$x \in \overline{y} \quad \Leftrightarrow \quad y \in \overline{x}.$$

(c) Soient $x, y \in E$. Si $y \in \overline{x}$, alors $\overline{y} = \overline{x}$.

(d) Soient x et y dans E. Alors on a : $xRy \Leftrightarrow \bar{x} = \bar{y}$.

(e) Soit $\overline{x}$ et $\overline{y}$ deux classes d'équivalence. Si $\overline{x} \cap \overline{y} \neq \emptyset$, alors $\overline{x} = \overline{y}$.

(f) L'ensemble des classes d'équivalences forme une partition *de E, c'est-à-dire :*

$$E = \bigsqcup_{\omega \in E/R} \omega.$$

(Rappelons que $\bigsqcup$ signifie la « réunion disjointe ».)

Démonstration. (a) Tout élément $x \in E$ appartient à la classe $\overline{x}$ par la réflexivité de la relation. Par définition, toute classe d'équivalence est de la forme $\overline{x}$, alors elle n'est pas vide.
(b) Nous avons les équivalences :

$$x \in \overline{y} \overset{\text{déf}}{\Leftrightarrow} yRx \overset{\text{symétrie}}{\Leftrightarrow} xRy \overset{\text{déf}}{\Leftrightarrow} y \in \overline{x}.$$

(c) Nous avons par définition $y \sim_R x$, et donc par la symétrie $x \sim_R y$. Prenons $y_1 \in \overline{y}$, donc $y \sim_R y_1$. La transitivité nous donne $x \sim_R y_1$; alors $y_1 \in \overline{x}$. Ceci montre $\overline{y} \subseteq \overline{x}$. Par (b) nous avons aussi $x \in \overline{y}$ et les mêmes arguments montrent $\overline{x} \subseteq \overline{y}$. Nous obtenons donc l'égalité $\overline{x} = \overline{y}$.
(d) « $\Leftarrow$ » est triviale. Pour « $\Rightarrow$ » on utilise (c).
(e) Soit $z \in \overline{x} \cap \overline{y}$, donc $z \in \overline{x}$ et $z \in \overline{y}$. Par (c) nous avons $\overline{z} = \overline{x}$ et $\overline{z} = \overline{y}$, donc $\overline{x} = \overline{y}$.
(f) et une conséquence directe de (a)–(e) : Il faut montrer

(1) que l'on a $E = \bigcup_{\omega \in E/R} \omega$ et

(2) que cette réunion est disjointe.

(1) est l'assertion (a) : tout élément de E appartient à une classe d'équivalence.
(2) est l'assertion (e) : deux classes d'équivalences sont soit les mêmes, soit disjointes. □

Proposition 5.17. *L'application de E dans E/R qui à tout élément x de E associe sa classe $\overline{x}$ est surjective ; on l'appelle* surjection canonique *de E dans E/R.*

En mathématiques, l'adjectif *canonique* est utilisé pour désigner un objet ou une construction naturelle, souvent définis de manière unique.

Démonstration. Appelons l'application s. Si $\overline{x}$ est une classe d'équivalence, alors $s(x) = \overline{x}$. Donc, on obtient la surjectivité. □

Factorisation canonique d'une application

Nous allons maintenant considérer un des exemples plus en détails. Soient E et F des ensembles et f une application de E dans F.

Vocabulaire 5.18. *Soient E un ensemble et A une partie de E ; on appelle* injection canonique de A dans E *l'application de A dans E qui envoie tout élément x de A sur x lui-même (vu comme élément de E).*

On note ici i l'injection canonique de $f(E)$ dans F et s la surjection canonique de E dans E/R_f.

Théorème 5.19. *Il existe une unique application bijective $\overline{f}$ de E/R_f dans $f(E)$ qui vérifie : $f = i \circ \overline{f} \circ s$.*

La relation vérifiée par les fonctions f, i, s et $\overline{f}$ peut s'écrire de manière compacte en disant que le *diagramme* suivant *commute*.

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ {\scriptstyle s}\downarrow & \circlearrowleft & \uparrow{\scriptstyle i} \\ E/R_f & \xrightarrow[\overline{f}]{\sim} & f(E) \end{array}$$

En règle générale, on note les applications surjectives par une flèche avec deux pointes $\twoheadrightarrow$, celles qui sont injectives par la flèche $\hookrightarrow$, et les bijections par une tilde au-dessus de la flèche $\xrightarrow{\sim}$.

Démonstration.

Unicité On considère deux applications, $\hat{f}$ et $\tilde{f}$ qui satisfont le théorème et on cherche à démontrer qu'elles sont égales.

Soient ω dans E/R_f une classe d'équivalence et x dans E un représentant de ω (c'est-à-dire qu'on a : $\omega = \overline{x} = s(x)$). Comme $\hat{f}$ et $\tilde{f}$ vérifient l'égalité $f = i \circ \hat{f} \circ s = i \circ \tilde{f} \circ s$, on a :

$$i\left(\hat{f}(\omega)\right) = i\left(\hat{f}(s(x))\right) = f(x) = i\left(\tilde{f}(s(x))\right) = i\left(\tilde{f}(\omega)\right).$$

Comme l'application i est injective, on en déduit : $\hat{f}(\omega) = \tilde{f}(\omega)$. Ceci étant valable pour toute classe ω dans E/R_f, on en conclut que $\hat{f}$ et $\tilde{f}$ sont égales.

Existence Soient ω dans E/R_f une classe d'équivalence et x dans E un représentant de ω. On pose $\overline{f}(\omega) = f(x)$.

Nous devons vérifier qu'on a bien construit ainsi une fonction $\overline{f}$, c'est-à-dire que la classe ω a une *unique* image par $\overline{f}$. Cette vérification est nécessaire car on a à priori défini $\overline{f}(\omega)$ à partir du choix d'un représentant x de ω, et pas seulement de ω lui-même.

Soit donc x' un autre représentant de la classe ω, c'est-à-dire qu'on a $x' \in \omega$ ou encore xR_fx'. Alors, par définition de la relation R_f, on a $f(x) = f(x')$. L'image de ω par $\overline{f}$ est donc bien définie (de manière unique). On dit que l'application f est « bien définie ».

On devra effectuer ce genre de vérification chaque fois qu'on veut définir une application sur un ensemble quotient.

L'application $\overline{f}$ est définie sur E/R_f et à valeurs dans $f(E)$. Nous allons démontrer qu'elle vérifie les propriétés du théorème.

Relation $f = i \circ \overline{f} \circ s$ Soit x dans E. Alors x est un représentant de sa classe d'équivalence $s(x)$ et on a par définition de $\overline{f}$: $(i \circ \overline{f} \circ s)(x) = i\left(\overline{f}(s(x))\right) = i\left(f(x)\right) = f(x)$.

Injectivité Soient ω et ω' des classes dans E/R_f vérifiant : $\overline{f}(\omega) = \overline{f}(\omega')$. Soient x un représentant de ω et x' un représentant de ω'. Alors on a : $f(x) = \overline{f}(\omega) = \overline{f}(\omega') = f(x')$. Ainsi, on a xR_fx', et donc $\omega = \overline{x} = \overline{x'} = \omega'$.

Surjectivité Soit y dans $f(E)$. Il existe x dans E vérifiant $y = f(x)$. Alors on a $y = f(x) = \overline{f}(s(x))$, donc y est dans l'image de $\overline{f}$.

□

Ainsi, toute application peut s'écrire comme composée d'une surjection, d'une bijection et d'une injection.

Chapitre II

Systèmes de nombres et structures algébriques

6 Les entiers naturels $\mathbb{N}$

Objectifs :

- Maîtriser les axiomes de Peano qui définissent les entiers naturels ;
- connaître la définition de l'addition, de la multiplication et de la relation d'ordre sur les entiers naturels ;
- savoir démontrer des propriétés simples.

Le but de cette section est d'esquisser la construction des nombres naturels. Jusqu'ici nous avons traité les entiers comme « connus (de l'école) ». Un des grands achèvements des mathématiques est de baser toutes les mathématiques sur une axiomatique fondamentale et de tout démontrer en partant des axiomes.
Pour vous en donner une idée, nous introduisons les axiomes de Peano qui définissent les nombres naturels. Par contre, nous n'avons pas le temps de donner toutes les démonstrations des propriétés « bien connues ». Une partie des détails sera donnée en appendice.

Les axiomes de Peano

Essayons maintenant d'oublier tout ce que nous savons sur les entiers naturels. Nous allons les définir de façon axiomatique et ensuite dériver toutes les propriétés « habituelles » en n'utilisant que les axiomes. Dans cette section il faut donc toujours justifier les règles de calculs par les axiomes ou des assertions déjà dérivées à partir des axiomes.

Définition 6.1. *On appelle* système des nombres naturels *tout triplet* $(N, S, 0)$ *consistant d'un ensemble* N*, d'une application* $S : N \to N$ *et d'un élément* $0 \in N$ *qui satisfait les trois axiomes (appelés* axiomes de Peano*) :*

(PA1) $0 \notin S(N)$,

(PA2) S *est injective,*

(PA3) $\forall\, M \subseteq N : \big(0 \in M \wedge (n \in M \Rightarrow S(n) \in M) \Rightarrow M = N\big)$.

L'application S est appelée *application de successeur*. L'idée est « $S(n) = n+1$ » (mais nous n'avons pas encore l'addition !). Juste pour montrer qu'il existe beaucoup de systèmes de nombres naturels, on mentionne qu'après avoir fait tout ce qui suit, on peut voir qu'un système des nombres naturels est par exemple donné par $(\{0, -1, -2, -3, \ldots\}, S, 0)$ avec $S(n) = n - 1$.

Théorème 6.2. *Dans l'axiomatique de la théorie des ensembles de Zermelo-Fraenkel, il existe un système des nombres naturels.*

Démonstration. Comme nous n'avons pas introduit les axiomes de Zermelo-Fraenkel, nous ne pouvons pas démontrer ce théorème et nous référons par exemple au livre de Schichl/Steinbauer, Section 6.1.1.
L'idée derrière la construction est la suivante :

- On pose $0 := \emptyset$.
- Pour $0 \neq n \in N$, on pose $S(n) = n \cup \{n\}$, la réunion de n (qui est un ensemble !) et l'ensemble dont le seul élément est l'ensemble n.

Plus explicitement :

$$0 = \emptyset,\ \ 1 = \{\emptyset\},\ \ 2 = \{\emptyset, \{\emptyset\}\},\ \ 3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\},\ \text{etc.}$$

□

A partir des axiomes de Peano nous démontrons maintenant le principe de récurrence que nous avons déjà utilisé (avec la phrase pas très convainquante « On s'en convainc que... »). Nous mettons donc les mathématiques que nous utilisons sur des fondations plus solides.

Proposition 6.3 (Principe de récurrence)**.** *Soit* $(N, S, 0)$ *un système des nombres naturels. Soit* $A(n)$ *une assertion dépendant de* n *dans* N*. Alors :*

$$(A(0) \wedge (\forall n \in N, A(n) \Rightarrow A(S(n)))) \Rightarrow (\forall\, n \in N, A(n)).$$

Démonstration. Nous définissons l'ensemble des nombres naturels pour lesquels l'assertion $A(n)$ est vraie :

$$V := \{n \mid n \in N, A(n)\}.$$

C'est un sous-ensemble de N. On a $0 \in V$ parce que $A(0)$ est vraie. Si $n \in V$, alors par définition $A(n)$ est vraie, donc $A(S(n))$ est vraie et en conséquence $S(n) \in V$. L'axiome (PA3) implique donc $V = N$, c'est-à-dire $A(n)$ est vraie pour tout $n \in N$. □

Lemme 6.4. *Soit* $(N, S, 0)$ *un système des nombres naturels. Alors,* $S(N) = N \backslash \{0\}$ *(tout* $n \in N \backslash \{0\}$ *est le successeur d'un élément dans* N*).*

Démonstration. Nous posons $M := S(N) \cup \{0\}$. C'est un sous-ensemble de N qui contient 0. Pour tout $m \in M$, on a $S(m) \in S(N) \subset M$. L'axiome (PA3) implique donc $M = N$. Comme (PA1) nous assure $0 \notin S(N)$, nous trouvons $S(N) = N \setminus \{0\}$. □

Lemme 6.5. *Soit $(N, S, 0)$ un système des nombres naturels. Alors, pour tout $n \in N$ nous avons $n \neq S(n)$.*

Démonstration. Exercice. □

Pour la suite, vous pouvez penser à l'exemple suivant : $E = \mathbb{R}$, $e = 2$ et $g(x) = x^2$; cela donne lieu à la définition récursive suivante :

$$f(0) = 2 \text{ et pour } n \in \mathbb{N} : f(n+1) = (f(n))^2$$

ou en notation de suites

$$a_0 = 2 \text{ et pour } n \in \mathbb{N} : a_{n+1} = (a_n)^2.$$

Proposition 6.6. *[Définitions récursives] Soit $(N, S, 0)$ un système des nombres naturels. Soient E un ensemble, $e \in E$ et $g : E \to E$ une application. Alors, il existe une unique application $f : N \to E$ telle que $f(0) = e$ et pour tout $n \in N$, $f(S(n)) = g(f(n))$.*

Démonstration. L'existence sera démontrée en appendice. Pour l'unicité on suppose que $\widetilde{f}$ est une deuxième application avec les mêmes propritétés que f. On considère l'ensemble

$$V := \{n \mid n \in N, f(n) = \widetilde{f}(n)\}.$$

Nous avons $0 \in V$ et si $n \in V$, alors $S(n) \in V$, parce que

$$f(S(n)) = g(f(n)) = g(\widetilde{f}(n)) = \widetilde{f}(S(n)),$$

donc par (PA3) $V = N$, montrant l'unicité. □

Proposition 6.7. *Si $(N, S, 0)$ et $(N', S', 0')$ sont des systèmes des nombres naturels, alors il existe une bijection $\varphi : N \to N'$ telle que $\varphi(0) = 0'$ et $\varphi \circ S = S' \circ \varphi$.*

Démonstration. Exercice. □

A cause de l'unicité dans la proposition 6.7, nous allons parler *des nombres naturels* et nous les notons $(\mathbb{N}, S, 0)$. Plus tard, nous n'allons qu'écrire $\mathbb{N}$.

Addition et multiplication

Nous définissons maintenant l'addition sur $(\mathbb{N}, S, 0)$.

Proposition 6.8. *Il existe une unique application*

$$f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad (m, n) \mapsto f(m, n) =: m + n$$

(noter que $m + n$ n'est qu'une façon d'écrire $f(m, n)$) telle que

(A1) $\forall\, m \in \mathbb{N} : m = f(m,0) = m + 0$,

(A2) $\forall\, m \in \mathbb{N}, \forall\, n \in \mathbb{N} : m + S(n) = f(m, S(n)) = S(f(m,n)) = S(m+n)$.

Démonstration. Soit $m \in \mathbb{N}$. La proposition 6.6 nous permet de définir l'application $f_m : \mathbb{N} \to \mathbb{N}$ récursivement par

$$f_m(0) := m \text{ et pour } n \in \mathbb{N} : \ f_m(S(n)) := S(f_m(n)).$$

Pour finir la preuve, nous posons $f(m,n) := f_m(n)$. Les deux propriétés sont satisfaites par construction.
On montre l'unicité. Supposons que nous avons deux fonctions f, f' ayant les propriétés de f. Nous définissons $f_m(n) := f(m,n)$ et $f'_m(n) := f'(m,n)$. Les propriétés (A1) et (A2) donnent $f_m(0) = m = f'_m(0)$ et $f_m(S(n)) = S(f_m(n))$ et $f'_m(S(n)) = S(f'_m(n))$. L'unicité dans la proposition 6.6 montre $f_m = f'_m$, donc $f = f'$. □

A cause de la proposition, nous pouvons maintenant écrire

$$S(n) = S(f(n,0)) = f(n, S(0)) = n + 1$$

avec $1 = S(0)$ (évidemment, on écrit $2 = S(1)$, $3 = S(2)$, etc.).

Proposition 6.9. *L'addition sur* $(\mathbb{N}, S, 0)$ *satisfait les propriétés suivantes. Pour tout* $m, n, \ell \in \mathbb{N}$ *on a*

(a) élément neutre : $m + 0 = m = 0 + m$ *;*

(b) commutativité : $m + n = n + m$ *;*

(c) associativité : $(m + n) + \ell = m + (n + \ell)$ *;*

(d) $\ell + n = m + n \Rightarrow \ell = m$ *;*

(e) $m + n = 0 \Leftrightarrow m = 0 \wedge n = 0$.

Démonstration. (a) $m + 0 = m$ est vrai par définition. L'égalité $m = 0 + m$ se démontre par récurrence. [Attention : nous ne connaissons pas encore la commutativité. C'est pour cela que l'assertion n'est pas triviale, mais nécessite une démonstration.]

Initialisation : $0 + 0 = f(0,0) = 0$.

Hérédité : « $m \Rightarrow m + 1$ » : $0 + (m+1) \overset{(A2)}{=} (0 + m) + 1 = m + 1$ où la dernière égalité utlise l'hypothèse de récurrence.

(b) On démontre d'abord :

$$(*) \quad \forall\, m, n \in \mathbb{N} : \ (m+1) + n = (m+n) + 1.$$

Soit $m \in \mathbb{N}$. Récurrence pour $n \in \mathbb{N}$:

Initialisation : $(m+1) + 0 \overset{(A1)}{=} m + 1 \overset{(A1)}{=} (m+0) + 1$.

Hérédité : « $n \Rightarrow n+1$ » : $(m+1)+(n+1) \overset{(A2)}{=} ((m+1)+n)+1 \overset{\text{hyp.réc.}}{=} ((m+n)+1)+1 \overset{(A2)}{=} (m+(n+1))+1$.

On démontre maintenant la commutativité aussi par récurrence pour $n \in \mathbb{N}$ avec $m \in \mathbb{N}$ fixé.

Initialisation : $m+0 = 0+m$ par (a).

Hérédité : « $n \Rightarrow n+1$ » : $m+(n+1) \overset{(A2)}{=} (m+n)+1 \overset{\text{hyp.réc.}}{=} (n+m)+1 \overset{(*)}{=} (n+1)+m$.

(c) Exercice.
(d) Récurrence pour n.

Initialisation : $m+0 = \ell+0$ donne $m = \ell$ à cause de (a).

Hérédité : « $n \Rightarrow n+1$ » : Supposons $m+(n+1) = \ell+(n+1)$. Par (A2) on a $(m+n)+1 = (\ell+n)+1$. Comme S est injective (PA2), on déduit $m+n = \ell+n$ et par l'hypothèse de récurrence $m = \ell$.

(e) L'implication $\Leftarrow$ est claire. Supposons donc $m+n = 0$ et faisons une démonstration par l'absurde. Pour cela on suppose (sans perte de généralité à cause de la commutativité de (b)) $n \neq 0$. Donc $n = \ell+1$ pour un $\ell \in \mathbb{N}$. En conséqence $0 = m+n = m+(\ell+1) \overset{(A2)}{=} (m+\ell)+1 = S(m+\ell)$ ce qui contredit $0 \notin S(N)$ (PA1). □

De façon similaire on définit une multiplication sur $\mathbb{N}$.

Proposition 6.10. *Il existe une unique application (appelée* multiplication*)*

$$g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad (m,n) \mapsto g(m,n) =: m \cdot n$$

(noter que $m \cdot n$ n'est qu'une façon d'écrire $g(m,n)$) telle que

(M1) $\forall\, m \in \mathbb{N} : 0 = g(m,0) = m \cdot 0$,

(M2) $\forall\, m \in \mathbb{N}, \forall\, n \in \mathbb{N} : m \cdot (n+1) = m \cdot S(n) = g(m,n) + m = m \cdot n + m$.

Esquisse de la démonstration. Soit $m \in \mathbb{N}$. La proposition 6.6 nous permet de définir l'application $g_m : \mathbb{N} \to \mathbb{N}$ récursivement par

$$g_m(0) := 0 \text{ et pour } n \in \mathbb{N} : \; g_m(S(n)) := g_m(n) + m.$$

Pour finir la preuve, nous posons $g(m,n) := g_m(n)$. Les deux propriétés sont satisfaites par construction. L'unicité se montre comme dans le cas de l'addition. □

Proposition 6.11. *La multiplication sur* $(\mathbb{N}, S, 0)$ *satisfait les propriétés suivantes.*
Pour tout $m, n, \ell \in \mathbb{N}$ *on a*

(a) élément neutre : $m \cdot 1 = m = 1 \cdot m$ *;*

(b) commutativité : $m \cdot n = n \cdot m$ *;*

(c) associativité : $(m \cdot n) \cdot \ell = m \cdot (n \cdot \ell)$ *;*

(d) $\ell \cdot n = m \cdot n \Rightarrow \ell = m \vee n = 0$ *;*

(e) intégrité : $m \cdot n = 0 \Rightarrow m = 0 \vee n = 0$ *;*

(f) distributivité : $(m + n) \cdot \ell = m \cdot \ell + n \cdot \ell$.

Démonstration. Similaire à la démonstration de la proposition 6.9. □

La relation d'ordre

Définition 6.12. *Soient* $m, n \in \mathbb{N}$. *On appelle* m plus petit ou égal à n *(*$m \leq n$*) s'il existe* $d \in \mathbb{N}$ *tel que* $m + d = n$.
L'entier naturel d *est appelé* la différence de n et m.

Lemme 6.13. *(a)* $\forall\, n \in \mathbb{N} : 0 \leq n$ *;*

(b) $\forall\, n \in \mathbb{N} : (n = 0 \vee 1 \leq n)$.

(c) $\forall\, n, m \in \mathbb{N} : (n \leq m \leq n + 1 \Rightarrow n = m \vee m = n + 1)$.

Démonstration. (a) Cela est vrai car $0 + n = n$.
(b) Supposons $n \leq 1$, alors il existe $d \in \mathbb{N}$ tel que $n + d = 1$. Si $d = 0$, alors $n = 1$. Si $d \neq 0$, alors $d = d' + 1$, donc $n + d' + 1 = 1$ et en conséquence $n + d' = 0$, alors $n = 0$ par la proposition 6.9 (e).
(c) $n \leq m$ implique l'existence de $d \in \mathbb{N}$ tel que $m = n + d$, donc $n \leq n + d \leq n + 1$, dont on déduit l'existence de $e \in \mathbb{N}$ tel que $n + d + e = n + 1$. La proposition 6.9 (d) nous donne $d + e = 1$, alors $d \leq 1$. La partie (b) implique $d = 0 \vee 1 \leq d$, donc $d = 0$ ou $d = 1$. □

Proposition 6.14. *La relation* $\leq$ *sur* $\mathbb{N}$ *est une relation d'ordre qui est totale. Elle satisfait en plus*

$$\ell \leq m \Rightarrow \forall\, n \in \mathbb{N} : (\ell + n \leq m + n \wedge \ell \cdot n \leq m \cdot n).$$

Démonstration. Nous démontrons uniquement la totalité. Soit $n \in \mathbb{N}$. Considérons l'ensemble

$$M = \{m \mid m \in \mathbb{N}, (n \leq m) \vee (m \leq n)\}.$$

A cause du lemme 6.13(a), nous avons $0 \in M$. Supposons maintenant $m \in M$. Si $n \leq m$, alors $n + d = m$ pour un $d \in \mathbb{N}$ et donc $n + (d + 1) = m + 1$ d'où $n \leq m + 1$, alors $m + 1 \in M$. Si $m \leq n$ et $m \neq n$, alors $m + d = n$ avec $d \in \mathbb{N}$ et $d \neq 0$, donc $d = d' + 1$, d'où $m + (d' + 1) = (m + 1) + d' = n$, alors $m + 1 \leq n$ et $m + 1 \in M$. Par (PA3) nous trouvons $M = \mathbb{N}$.
Les autres assertions se vérifient facilement ; nous ne donnons pas les détails ici. C'est un exercice instructif. □

La relation d'ordre nous permet de démontrer que $\mathbb{N}$ est *bien ordonné*.

Proposition 6.15 ($\mathbb{N}$ est bien ordonné)**.** *Toute partie* M *non vide de* $\mathbb{N}$ *possède un plus petit élément.*

Démonstration. Par récurrence. Soit $A(n)$ l'assertion : « toute partie $M \subseteq \mathbb{N}$ telle que $n \in M$ possède un plus petit élément ».

Initialisation : $A(0)$ est vraie car 0 est le plus petit élément de $\mathbb{N}$ par le lemme 6.13.

Hérédité : « $A(n) \Rightarrow A(n+1)$ » : On distingue deux cas.

1er cas : $n \in M$: on peut appliquer $A(n)$ pour conclure que M possède un plus petit élément.

2ème cas : $n \notin M$: On considère $M' = M \cup \{n\}$. En appliquant $A(n)$ on obtient que M' possède un plus petit élément, appelons-le x. Si $x < n$, alors x est aussi le plus petit élément de M. Si $x = n$, alors $n+1$ est le plus petit élément de M par le lemme 6.13.

□

En fait, on peut aussi déduire le principe de récurrence de la proposition 6.15 comme suit :

> On suppose que les assertions $A(0)$ et $(\forall n \in \mathbb{N}, A(n) \Rightarrow A(n+1))$ sont vraies ; on veut démontrer que, pour tout n dans $\mathbb{N}$, l'assertion $A(n)$ est vraie. On suppose par l'absurde que ce n'est pas le cas.
>
> La négation de $(\forall n \in \mathbb{N}, A(n))$ est : il existe n dans $\mathbb{N}$ pour lequel l'assertion $A(n)$ est fausse. On considère alors l'ensemble $\mathcal{A}$ des entiers naturels m tels que l'assertion $A(m)$ est fausse. Par hypothèse, l'ensemble $\mathcal{A}$ est non vide. Comme $\mathbb{N}$ est bien ordonné, $\mathcal{A}$ possède un plus petit élément ; notons le m_0. On remarque que, comme m_0 appartient à $\mathcal{A}$, l'assertion $A(m_0)$ est fausse.
>
> Comme $A(0)$ est vraie, $\mathcal{A}$ ne contient pas 0, donc m_0 est non nul. On peut donc considérer l'entier naturel $m_0 - 1$, qui est strictement inférieur à m_0 ; comme tous les éléments de $\mathcal{A}$ sont plus grands que m_0, l'entier $m_0 - 1$ n'appartient pas a $\mathcal{A}$. Ainsi, la propriété $A(m_0 - 1)$ est vraie. Alors, la propriété $A(m_0 - 1 + 1) = A(m_0)$ est vraie. On obtient une contradiction.

La propriété de bon ordre de $\mathbb{N}$ a également les deux conséquences suivantes.

Proposition 6.16. *Toute partie non vide et majorée de* $\mathbb{N}$ *admet un plus grand élément.*

Démonstration. Soit $\mathcal{A}$ une partie non vide et majorée de $\mathbb{N}$.
On considère l'ensemble $\mathcal{M}$ des majorants de $\mathcal{A}$, c'est-à-dire l'ensemble :

$$\mathcal{M} = \{m \in \mathbb{N} \mid \forall a \in \mathcal{A}, a \leq m\}.$$

Par hypothèse ($\mathcal{A}$ est majorée), la partie $\mathcal{M}$ est non vide.
Soit m_0 le plus petit élément de $\mathcal{M}$. Si m_0 est dans $\mathcal{A}$, alors c'est le plus grand élément de $\mathcal{A}$.
On suppose par l'absurde que m_0 n'est pas dans $\mathcal{A}$. Alors pour tout a dans $\mathcal{A}$ ($\mathcal{A}$ est non vide), on a $a \leq m_0$ et $a \neq m_0$, donc $a < m_0$ et par suite $a \leq m_0 - 1$. Ainsi, l'entier $m_0 - 1$ est aussi un majorant de $\mathcal{A}$; il appartient donc à $\mathcal{M}$, ce qui contredit le choix de m_0 comme plus petit élément de $\mathcal{M}$. □

À partir des entiers naturels $\mathbb{N}$ et de relations d'équivalence sur des ensembles bien choisis, on construira dans la suite du cours les entiers relatifs $\mathbb{Z}$ et les nombres rationnels $\mathbb{Q}$ avec leurs propriétés usuelles.
Nous sommes à présent plus sûrs des fondations, et à partir de maintenant, nous allons travailler avec les nombres naturels comme nous l'avons toujours fait.

Appendice : Quelques détails

Cet appendice ne sera pas traité en cours.

Justification des définitions récursives

On commence par les parties initiales (il faut se les imaginer comme $\{0, 1, 2, \ldots, n\}$).

Définition 6.17. *Soit $(N, S, 0)$ un système des nombres naturels. Un sous-ensemble $I \subseteq N$ est appelé* partie initiale *si pour tout $i \in N$*

$$i \notin I \Rightarrow S(i) \notin I$$

ou équivalant : $S(i) \in I \Rightarrow i \in I$.

Lemme 6.18. *Soit $(N, S, 0)$ un système des nombres naturels.*

(a) Soit $\emptyset \neq I \subseteq N$ une partie initiale. Alors $0 \in I$.

(b) Pour tout $n \in N$ il existe une partie initiale I_n telle que $n \in I_n$ et $S(n) \notin I_n$ et satisfaisant $I_0 = \{0\}$ et $I_{S(n)} = I_n \sqcup \{S(n)\}$ pour tout $n \in N$. (Il faut s'imaginer I_n comme $\{0, 1, 2, \ldots, n-1, n\}$.)

(c) $\bigcup_{n \in N} I_n = N$.

Démonstration. (a) Supposons le contraire : $0 \notin I$. Soit $C := N \setminus I$ le complément. On a $0 \in C$ et $n \in C \Rightarrow S(n) \in C$, donc $C = N$ par l'axiome (PA3), donc $I = \emptyset$, contradiction.
(b) Par récurrence. Soit $A(n)$ l'assertion de l'existence d'une partie initiale I_n avec $n \in I_n$ et $S(n) \notin I_n$.

Initialisation : Pour $n = 0$ on pose $I_0 = \{0\}$. Evidemment $0 \in I_0$ et $S(0) \notin I_0$. En plus, I_0 est une partie initiale car (PA1) nous assure que 0 n'est pas dans $S(N)$.

Hérédité : « $A(n) \Rightarrow A(S(n))$ » : On pose $I_{S(n)} := I_n \cup \{S(n)\}$. La réunion est en fait disjointe car $S(n) \in I_n$ contredirait $A(n)$. Il est clair que $S(n) \in I_{S(n)}$. En plus, $I_{S(n)}$ est une partie initiale : si $S(m) \in I_n$, alors $m \in I_n \subset I_{S(n)}$ car I_n est une partie initiale ; si $S(m) = S(n)$, alors $m = n \in I_n \subset I_{S(n)}$.

Il reste à voir que $S(S(n)) \notin I_{S(n)}$. Supposons le contraire : $S(S(n)) \in I_{S(n)}$. Comme l'injectivité de S (PA2) exclut $S(S(n)) = S(n)$ à cause du lemme 6.5, on suppose $S(S(n)) \in I_n$; alors, comme I_n est une partie initiale, on aurait $S(n) \in I_n$, contradiction avec l'hypothèse $A(n)$.

Conclusion : Pour tout $n \in N$ l'assertion $A(n)$ est vraie, donc la partie (b) est vraie.

La deuxième assertion résulte de la construction.
(c) L'inclusion « $\subseteq$ » est triviale. L'inclusion « $\supseteq$ » résulte de $n \in I_n$. □

Démonstration de la partie « existence » dans la proposition 6.6. Par récurrence, nous allons démontrer l'assertion suivante :

$$A(n) : \ \exists f_n : I_n \to E : \ f_n(0) = e \wedge \big(\forall\, m \in N : (S(m) \in I_n \Rightarrow f_n(S(m)) = g(f_n(m))\big).$$

Initialisation : Pour $n = 0$ on pose $f_0(0) = e$. L'existence est donc claire car $I_0 = \{0\}$.

Hérédité : « $A(n) \Rightarrow A(S(n))$ » : On se rappelle que $I_{S(n)} = I_n \sqcup \{S(n)\}$. On pose

$$f_{S(n)}(m) := \begin{cases} f_n(m) & \text{si } m \in I_n, \\ g(f_n(n)) & \text{si } m = S(n). \end{cases}$$

Il faut vérifier les propriétés :

- $f_{S(n)}(0) = f_n(0) = e$ par l'hypothèse de récurrence.
- Soit $m \in N$ tel que $S(m) \in I_{S(n)}$. Pour $m = n$, on a $f_{S(n)}(S(n)) = g(f_n(n)) = g(f_{S(n)}(n))$ par définition. Pour $m \neq n$, on a $f_{S(n)}(S(m)) = f_n(S(m)) = g(f_n(m)) = g(f_{S(n)}(m))$ par l'hypothèse de récurrence.

Nous allons maintenant définir l'application f pour $n \in N$ comme

$$f(n) := f_n(n).$$

Elle satisfait

- $f(0) = f_0(0) = e$,
- pour $n \in N$ on a $f(S(n)) = f_{S(n)}(S(n)) = g(f_n(n)) = g(f(n))$.

Nous avons montré l'existence à cause de $N = S(N) \cup \{0\}$ (lemme 6.4). □

Lemme 6.19. *Pour tout $n \in \mathbb{N}$, nous avons $I_n = \{m \mid m \in \mathbb{N}, m \leq n\}$.*

Démonstration. « $\subseteq$ » : Considérons l'ensemble $M = I_n \cap \{m \mid m \in \mathbb{N}, m > n\}$. Si $M \neq \emptyset$, alors M possède un plus petit élément x. Comme $n+1 \notin I_n$, on a $x > n+1$ et $x = y+1$ avec $y \in \mathbb{N}$ et $y > n$. Le fait $y + 1 \in I_n$ implique $y \in I_n$ car I_n est une partie initiale. On trouve $y \in M$, contradiction car $y < x$ et x est le plus petit élément de M. Donc, M est l'ensemble vide et $I_n \subseteq \{m \mid m \in \mathbb{N}, m \leq n\}$. « $\supseteq$ » : Considérons l'ensemble $M = \{m \mid m \in \mathbb{N}, m \leq n\} \setminus I_n$. C'est un ensemble majoré. Supposons M non-vide. Donc M possède un plus grand élément x ; on a $x \leq n$ et $x \notin I_n$. En fait, $x < n$ car $n \in I_n$. En conséquence, $x + 1 \notin I_n$ car I_n est une partie initiale et $x + 1 \leq n$. On trouve $x + 1 \in M$. Cela contradit la maximalité de x. Donc M est l'ensemble vide et $\{m \mid m \in \mathbb{N}, m \leq n\} \subseteq I_n$. □

Nous avons donc pour tout $n, m \in \mathbb{N}$:

$$n \leq m \Leftrightarrow I_n \subseteq I_m.$$

Le cardinal d'un ensemble

Ici nous donnons une formalisation du cardinal d'un ensemble. Soit E un ensemble. Nous avons déjà introduit le symbole $\#E$ pour noter le nombre d'éléments de E. Nous allons formaliser cette notion.

Définition 6.20. *Pour tout $n \in \mathbb{N}$ on note $E_n := I_n \setminus \{0\} = \{1, 2, \ldots, n\}$, en particulier, $E_0 = \emptyset$.*
Soit E un ensemble. Il est appelé fini *s'il existe $n \in \mathbb{N}$ et une bijection $\varphi : E_n \to E$. Dans ce cas, on dit que le nombre d'éléments $\#E$ (ou : $|E|$) de E (ou : le* cardinal*) est égal à n.*
Soient E, F des ensembles (pas nécessairement finis). On dit que E et F ont le même cardinal *s'il existe une application bijective $f : E \to F$.*
Les ensembles qui ont le même cardinal que $\mathbb{N}$ sont appelés dénombrables.

Noter que pour $n, m \in \mathbb{N}$ on a

$$n \leq m \Leftrightarrow E_n \subseteq E_m.$$

Exemple 6.21.

- $|\emptyset| = 0$ *(est $\emptyset$ est le seul ensemble de cardinal 0),* $|\{1\}| = 1$, $|\{A, B\}| = 2$.
- *Les nombres pairs sont dénombrables :*

  $$\mathbb{N} \xrightarrow{n \mapsto 2n} \{2n \mid n \in \mathbb{N}\}$$

  est une bijection.
- $\mathbb{N} \times \mathbb{N}$ *est dénombrable (voir l'exercice 4.8(c)).*
- $\mathbb{Z}$ *est dénombrable car*

  $$\mathbb{N} \longrightarrow \mathbb{Z}, n \mapsto \begin{cases} 0 \mapsto 0, \\ n \mapsto \frac{n+1}{2} \text{ si } n \text{ est impair}, \\ n \mapsto -\frac{n}{2} \text{ si } n \text{ est pair} \end{cases}$$

  est une bijection.
- $\mathbb{R}$ *n'est pas dénombrable par l'argument de la diagonale de Cantor (voir à propos sur feuille d'exercices).*

Lemme 6.22. *Soient $n, m \in \mathbb{N}$ deux nombres naturels distincts. Alors pour tout $m > n$, il n'existe pas d'injection $E_m \hookrightarrow E_n$.*

Démonstration. For $n \in \mathbb{N}$, on considère l'assertion

$$A(n) : \forall\, m > n : \text{ Il n'existe pas d'injection } E_m \to E_n.$$

Nous la démontrons par récurrence.

Initialisation Pour $n = 0$, on a $E_n = \emptyset$ et $m \in E_m \neq \emptyset$ pour tout $m > 0$. Il n'existe donc pas d'injection $E_m \to E_0$ (il n'existe même pas d'application).

Hérédité Supposons $A(n)$ vrai. Soit $m' = m + 1 > n + 1$. Supposons que nous avons une injection $\varphi : E_{m+1} \to E_{n+1}$.

1er cas. $n+1 \notin \mathrm{im}(\varphi)$. Alors φ se restreint pour donner une injection $E_{m'} \to E_n$, contradiction.

2ème cas. $n+1 \in \mathrm{im}(\varphi)$. Alors il existe $a \in E_{m+1}$ tel que $\varphi(a) = n+1$. Nous modifions l'injection φ comme suit

$$\varphi' : E_{m+1} \to E_{n+1}, \quad x \mapsto \begin{cases} \varphi(x) & \text{si } x \neq m+1 \wedge x \neq a, \\ n+1 & \text{si } x = m+1, \\ \varphi(m+1) & \text{si } x = a. \end{cases} .$$

L'application φ' est une injection et satisfait $\varphi'(m+1) = n+1$. Donc elle se restreint pour donner une injection $E_m \to E_n$, contradiction. L'assertion $A(n+1)$ suit.

□

Proposition 6.23. *Soient E, F deux ensembles finis. Alors :*

(a) $\#E = \#F \Leftrightarrow$ il existe une bijection $f : E \to F$.

(b) $\#E \leq \#F \Leftrightarrow$ il existe une injection de E dans F.

(c) $\#F \leq \#E \Leftrightarrow$ il existe une surjection de E dans F.

Ce résultat sera utilisé très souvent pour calculer le cardinal d'un ensemble F : on trouvera une bijection entre cet ensemble et un ensemble E dont on connaît déjà le cardinal.

Démonstration. Soient $m := \#E$ et $n := \#F$. Par définition il existe des bijections $g : E_m \to E$ et $h : E_n \to F$. Notons g^{-1} l'inverse de g et h^{-1} l'inverse de h.
(a) « $\Rightarrow$ » : Comme $n = m$ on peut former la composée

$$E \xrightarrow{g^{-1}} E_n = E_m \xrightarrow{h} F$$

qui est une bijection car c'est la composée de deux bijections.
« $\Leftarrow$ » : Supposons que $f : E \to F$ est une bijection. Donc, la composée

$$E_n \xrightarrow{g} E \xrightarrow{f} F \xrightarrow{h^{-1}} E_m$$

est une bijection. Par le lemme 6.22 on obtient $n \leq m$. La même argumentation avec f^{-1} donne $m \leq n$, donc $n = m$.
(b) « $\Rightarrow$ » : Comme $n = m$ on peut former la composée

$$E \xrightarrow{g^{-1}} E_n \hookrightarrow E_m \xrightarrow{h} F$$

où $E_n \hookrightarrow E_m$ est l'inclusion. La composée est une injection car c'est la composée d'injections.
« $\Leftarrow$ » : Comme (a).
(c) Exercice. □

Voici encore un résumé de quelques propriétés utiles d'ensembles finis.

Proposition 6.24. *Soient E, F des ensembles finis. Alors :*

(a) Toute partie A de E est finie et vérifie $|A| \leq |E|$. Si on a de plus $|A| = |E|$, alors $A = E$.

(b) $E \cup F$ est fini. Si $E \cap F = \emptyset$, alors $|E \sqcup F| = |E| + |F|$. En général, $|E \cup F| = |E| + |F| - |E \cap F|$.

(c) $E \times F$ est fini et $|E \times F| = |E| \cdot |F|$.

(d) Soit $\mathcal{F}(E, F)$ l'ensemble de toutes les applications de E dans F. C'est un ensemble fini et $|\mathcal{F}(E, F)| = |F|^{|E|}$.

(e) $\mathcal{P}(E)$ est fini et $|\mathcal{P}(E)| = 2^{|E|}$.

(f) L'ensemble $\mathcal{S}(E)$ des bijections de E dans lui-même est fini et on a $|\mathcal{S}(E)| = |E|!$ ($|E|$ factorielle).

(g) Soit f une fonction de E dans F. Alors $|f(E)| \leq \min(|E|, |F|)$. On a $|f(E)| = |E|$ si et seulement si f est injective et $|f(F)| = |F|$ si et seulement si f est surjective.

Démonstration. C'est un bon exercice de démontrer les parties qui n'ont pas été traitées. □

7 Groupes

Objectifs :

- Apprendre et maîtriser la définition de groupes ;
- connaître et savoir calculer dans le groupe symétrique ;
- savoir démontrer des propriétés simples.

Le monoïde $(\mathbb{N}, +, 0)$

Les propriétés suivantes des nombres naturels ont été démontrées dans la proposition 6.9.

Associativité : $\forall\, n_1, n_2, n_3 \in \mathbb{N} :\ (n_1 + n_2) + n_3 = n_1 + (n_2 + n_3)$.

Élément neutre : $\forall\, n \in \mathbb{N} : 0 + n = n + 0 = n$.

Commutativité : $\forall\, n_1, n_2 \in \mathbb{N} : n_1 + n_2 = n_2 + n_1$.

Définition 7.1. *Soient G un ensemble, $e \in G$ un élément et*

$$* : G \times G \to G$$

une application. On appelle le triplet $(G, *, e)$ un monoïde *si*

Associativité : $\forall\, g_1, g_2, g_3 \in G :\ (g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$ *;*

Élément neutre : $\forall\, g \in G : e * g = g * e = g$.

Un monoïde $(G, *, e)$ est appelé commutatif *ou* abélien *si*

Commutativité : $\forall\, g_1, g_2 \in G : g_1 * g_2 = g_2 * g_1$.

Donc $(\mathbb{N}, +, 0)$ est un monoïde commutatif.

Lemme 7.2. *Soit $(G, *, e)$ un monoïde. Le seul élément f de G tel que pour tout $g \in G$ on a $f * g = g * f = g$ est e.*

Démonstration. $e = f * e = f$. □

Le groupe symétrique

Soit M un ensemble fini.

Notation 7.3.

$$S_M := \{f \mid f : M \to M \text{ application bijective } \}$$

Si $M = \{1, 2, \ldots, n\}$, alors on note $S_M =: S_n$.

Nous rappelons que le cardinal de S_n est $n!$.
Rappelons que nous avons déjà démontré *l'associativité de la composition d'applications* dans le lemme 4.5. Dans notre cas c'est : soient $f, g, h \in S_M$; alors

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Nous avons aussi défini *l'identité,* $\mathrm{id} : M \to M$*,* $m \mapsto m$. Elle satisfait :

$$\forall\, f \in S_M :\ \mathrm{id} \circ f = f \circ \mathrm{id} = f.$$

Donc, $(S_M, \circ, \mathrm{id})$ est un monoïde.
Dès que M a au moins trois éléments S_M **n'est pas commutatif** : Soient, par exemple, $M = \{1, 2, 3\}$ et $f(1) = 2$, $f(2) = 3$, $f(3) = 1$ et $g(1) = 2$, $g(2) = 1$, $g(3) = 3$; donc :

$$f \circ g(1) = 3,\ \ f \circ g(2) = 2,\ \ f \circ g(3) = 1 \text{ mais } g \circ f(1) = 1,\ \ g \circ f(2) = 3,\ \ g \circ f(3) = 2.$$

Mais S_M satisfait une autre propriété très importante : *l'existence d'inverse* que nous connaissons aussi déjà du lemme 4.6. Pour tout $f \in S_M$ il existe $g \in S_M$ tel que $f \circ g = g \circ f = \mathrm{id}$.

Définition de groupe et propriétés

Nous sommes menés par ces considérations à la définition d'un groupe :

Définition 7.4. *Soit $(G, *, e)$ un monoïde. Il est appelé un* groupe *si*

Existence d'inverse : $\forall\, g \in G\ \exists\, h \in G : h * g = g * h = e$.

Si un groupe $(G, *, e)$ est commutatif (en tant que monoïde), on parle d'un groupe abélien.

Donc, S_M est un groupe. On appelle S_n le *groupe symétrique (en n lettres)*.
Attention : $(\mathbb{N}, +, 0)$ n'est pas un groupe car les inverses n'existent pas.
Par contre $(\mathbb{Z}, +, 0)$ est un groupe : l'élément inverse de $m \in \mathbb{Z}$ est $-m$ car

$$0 = (-m) + m = m + (-m).$$

Alors, $(\mathbb{Z}, +, 0)$ est un groupe abélien.

Lemme 7.5. *Soit $(G, *, e)$ un groupe et $g \in G$. L'inverse de g est unique : Si $h_1, h_2 \in G$ vérifient $h_i * g = g * h_i = e$ pour $i = 1, 2$, alors $h_1 = h_2$.*

Démonstration. $h_1 \overset{\text{élém. neutre}}{=} e * h_1 = (h_2 * g) * h_1 \overset{\text{associativité}}{=} h_2 * (g * h_1) = h_2 * e \overset{\text{élém. neutre}}{=} h_2$. □

Lemme 7.6. *Soit $(G, *, e)$ un groupe et $g, h \in G$. Soient g^{-1} l'inverse de g et h^{-1} l'inverse de h. Alors, l'inverse de $g * h$ est $h^{-1} * g^{-1}$.*

Démonstration. $(g * h) * (h^{-1} * g^{-1}) = g * (h * h^{-1}) * g^{-1} = g * e * g^{-1} = g * g^{-1} = e$ et $(h^{-1} * g^{-1}) * (g * h) = h^{-1} * (g^{-1} * g) * h = h^{-1} * e * h = h^{-1} * h = e$. □

Les éléments du groupe symétrique

On présente deux manières pour noter les éléments f de S_n. Voici la première :

$$f = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ f(1) & f(2) & f(3) & \dots & f(n-1) & f(n) \end{pmatrix}.$$

Par exemple, si $n = 4$ et $f(1) = 2$, $f(2) = 4$, $f(3) = 3$, $f(4) = 1$, alors

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}.$$

Beaucoup plus pratique, mais un peu plus difficile au début, est la deuxième manière, l'écriture en *cycles à supports disjoints*. Avant de l'expliquer il nous faut démontrer un lemme :

Lemme 7.7. *Soit $m \in M$ (fini). Il existe un $n \in \mathbb{N}_{>0}$ tel que $f^n(m) := \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ fois}}(m) = m$.*

Démonstration. Pour tout $n \in \mathbb{N}_{>0}$, l'élément $f^n(m)$ appartient à l'ensemble fini M. Donc, il existe $n_1 \neq n_2$ tels que $f^{n_1}(m) = f^{n_2}(m)$. Supposons sans perte de généralité que $n_1 > n_2$ et écrivons $n := n_1 - n_2$. Donc

$$f^{n_2}(m) = f^{n_1}(m) = f^{n_2} \circ f^n(m).$$

Soit $g \in S_M$ l'inverse de f^{n_2}, alors

$$m = g \circ f^{n_2}(m) = g \circ (f^{n_2} \circ f^n(m)) = (g \circ f^{n_2}) \circ f^n(m) = \mathrm{id} \circ f^n(m) = f^n(m).$$

La démontration est achevée. □

Nous notons f^{-1} l'inverse de f dans S_M.
Soit $m \in M$, $f \in S_M$ et $n \in \mathbb{N}_{>0}$ le plus petit entier naturel non nul tel que $f^n(m) = m$. Donc, $f^{-1}(m) = f^{n-1}(m)$. Le cycle de f qui contient m est défini comme :

$$\big(m \;\; f(m) \;\; f^2(m) \;\; f^3(m) \;\; \ldots \;\; f^{n-1}(m)\big).$$

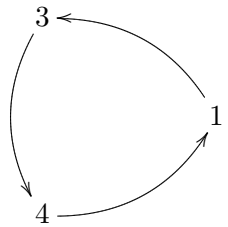
Exemple 7.8. *(a)* $M = \{1, 2, 3, 4, 5, 6\}$.

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 5 & 2 \end{pmatrix}.$$

Le cycle qui contient 1 *est* $\big(1 \;\; 3 \;\; 4\big)$. *C'est évidemment aussi le cycle qui contient* 3 *et* 4. *Encore une fois, la signification de ce cycle est :*

$$1 \mapsto 3, \quad 3 \mapsto 4, \quad 4 \mapsto 1.$$

Alors, on voit le cycle vraiment comme un cycle (il n'y a ni début ni fin) : on peut se le représenter en écrivant les élément sur un cercle :



Donc on peut l'écrire aussi comme : $\big(3 \;\; 4 \;\; 1\big)$ *et* $\big(4 \;\; 1 \;\; 3\big)$. *(Attention ! Le cycle* $\big(1 \;\; 4 \;\; 3\big)$ *est différent : il représente l'application* $1 \mapsto 4, \quad 4 \mapsto 3, \quad 3 \mapsto 1$.*)*

Le cycle qui contient 2 *est* $\big(2 \;\; 6\big)$, *et le cycle qui contient* 5 *est* $\big(5\big)$.

L'écriture en cycles de f *est*

$$f = \big(1 \;\; 3 \;\; 4\big) \; \big(2 \;\; 6\big) \; \big(5\big).$$

Souvent on n'écrit pas les cycles qui n'ont qu'un seul élément (sauf l'identité qui s'écrit $\mathrm{id} = \big(1\big)$*), alors*

$$f = \big(1 \;\; 3 \;\; 4\big) \; \big(2 \;\; 6\big).$$

(b) Voici la liste complète des éléments de S_3 *:*

$$\big(1\big), \;\; \big(1 \;\; 2\big), \;\; \big(1 \;\; 3\big), \;\; \big(2 \;\; 3\big), \;\; \big(1 \;\; 2 \;\; 3\big), \;\; \big(1 \;\; 3 \;\; 2\big).$$

(c) La composition de deux éléments en écriture en cycles (et, pour la dernière fois, autrement) :

$$\begin{aligned} \big(1 \;\; 6 \;\; 3 \;\; 5\big) \; \big(2 \;\; 4\big) \circ \big(1 \;\; 3 \;\; 4\big) \; \big(2 \;\; 6\big) \qquad &= \big(1 \;\; 5\big) \; \big(2 \;\; 3\big) \; \big(4 \;\; 6\big) \\ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 5 & 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 5 & 2 \end{pmatrix} \qquad &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 2 & 6 & 1 & 4 \end{pmatrix}. \end{aligned}$$

(d) L'inverse de $\begin{pmatrix}1 & 6 & 3 & 5\end{pmatrix}\begin{pmatrix}2 & 4\end{pmatrix} \in S_6$ *est* $\begin{pmatrix}1 & 5 & 3 & 6\end{pmatrix}\begin{pmatrix}2 & 4\end{pmatrix}$*. Donc pour obtenir l'inverse, on écrit les cycles en sense inverse.*

Définition 7.9.

(a) On appelle cycle *toute permutation* σ *dans* S_n *telle qu'il existe* k *compris entre* 1 *et* n*, et des entiers* $a_1, ..., a_k$ *dans* $\{1, ..., n\}$*, deux à deux distincts, tels que* $\sigma = (a_1 \dots a_k)$*.*

(b) L'entier k *et l'ensemble* $\{a_1, ..., a_k\}$ *sont alors uniques ;* k *est appelé la* longueur *du cycle et* $\{a_1, ..., a_k\}$ *est appelé le* support *du cycle.*

(c) Deux cycles sont dits à supports disjoints *si l'intersection de leurs supports est vide.*

Remarque 7.10. *(a) On rappelle que, lorsque l'on écrit un cycle, on peut commencer par n'importe quel élément du support (en respectant ensuite l'ordre des* a_i*). On a par exemple :*

$$(1635) = (6351) = (3516) = (5163).$$

(b) Deux cycles à supports disjoints commutent. Cela est un exercice facile.

(c) Attention, deux cycles dont les supports sont non disjoints ne commutent pas toujours. On a par exemple dans S_3 *:*

$$(12)(23) = (123) \neq (132) = (23)(12).$$

(d) Toute permutation de S_n *s'écrit comme produit de cycles à supports disjoints. Cette écriture est unique, à l'ordre des cycles près.*

On a par exemples les égalités :

$$\begin{pmatrix}1 & 6 & 3 & 5\end{pmatrix}\begin{pmatrix}2 & 4\end{pmatrix} = \begin{pmatrix}2 & 4\end{pmatrix}\begin{pmatrix}1 & 6 & 3 & 5\end{pmatrix} = \begin{pmatrix}4 & 2\end{pmatrix}\begin{pmatrix}3 & 5 & 1 & 6\end{pmatrix}.$$

Définition 7.11. *Un élément* $\tau \in S_n$ *est appelé* transposition *s'il existe* $i, j \in \{1, 2, \dots, n\}$*,* $i \neq j$ *tels que* $\tau = \begin{pmatrix}i & j\end{pmatrix}$*.*

Proposition 7.12. *Le groupe symétrique* S_n *est engendré par ses transpositions, c'est-à-dire, tout élément peut s'écrire comme produit de transpositions.*

Démonstration. Il suffit de montrer que tout cycle $\begin{pmatrix}a_1 & a_2 & a_3 \dots a_r\end{pmatrix}$ s'écrit comme un produit de transpositions. C'est le cas car :

$$\begin{pmatrix}a_1 & a_2 & a_3 \dots a_r\end{pmatrix} = \begin{pmatrix}a_r & a_1\end{pmatrix} \circ \begin{pmatrix}a_{r-1} & a_1\end{pmatrix} \circ \cdots \circ \begin{pmatrix}a_3 & a_1\end{pmatrix} \circ \begin{pmatrix}a_2 & a_1\end{pmatrix}.$$

□

8 Anneaux

Objectifs :

- Maîtriser la notion d'anneau ;
- connaître des exemples d'anneaux ;
- maîtriser les notions de diviseur de zéro et d'unité ;
- savoir démontrer des propriétés simples.

Les entiers relatifs $\mathbb{Z}$ sont un ensemble avec deux lois, l'addition et la multiplication,

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (a, b) \mapsto a + b,$$
$$\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (a, b) \mapsto a \cdot b,$$

et deux éléments spéciaux 0, 1 tels que

- ($(\mathbb{Z}, +, 0)$ est un groupe abélien) : pour tout $\ell, m, n \in \mathbb{Z}$:
  - *élément neutre :* $m + 0 = m = 0 + m$;
  - *associativité :* $(m + n) + \ell = m + (n + \ell)$;
  - *existence d'inverse :* $m + (-m) = 0 = (-m) + m$;
  - *commutativité :* $m + n = n + m$.
- ($(\mathbb{Z}, \cdot, 1)$ est un monoïde commutatif) : pour tout $\ell, m, n \in \mathbb{Z}$:
  - *élément neutre :* $m \cdot 1 = m = 1 \cdot m$;
  - *associativité :* $(m \cdot n) \cdot \ell = m \cdot (n \cdot \ell)$;
  - *commutativité :* $m \cdot n = n \cdot m$.
- (relation entre $+$ et $\cdot$) :
  - *distributivité :* $(m + n) \cdot \ell = m \cdot \ell + n \cdot \ell$.

Comme vous le savez sans doute, les mêmes opérations existent par exemple pour les nombres rationnels, les nombres réels et les nombres complexes. Cela nous amène à donner un nom spécial aux ensembles ayant de telles structures : *anneau*.

Définition 8.1. *Soient A un ensemble, $0_A, 1_A \in A$ deux éléments (pas nécessairement distincts) et*

$$+_A : A \times A \to A, \quad \text{et} \quad \cdot_A : A \times A \to A$$

deux applications. On appelle le tuplet $(A, +_A, \cdot_A, 0_A, 1_A)$ un anneau (commutatif) *si*

- $(A, +_A, 0_A)$ *est un groupe abélien,*
- $(A, \cdot_A, 1_A)$ *est un monoïde (commutatif) et*

- *pour tous* $a, b, c \in A$ *:*

$$a \cdot_A (b +_A c) = (a \cdot_A b) +_A (a \cdot_A c)$$

et

$$(a +_A b) \cdot_A c = (a \cdot_A c) +_A (b \cdot_A c)$$

*(*distributivité).

Donc, $(\mathbb{Z}, +, \cdot, 0, 1)$ est un anneau commutatif. On le notera souvent juste $\mathbb{Z}$.
Notez que si l'anneau est commutatif (par définition la multiplication est commutative), il suffit de vérifier une seule des deux égalités pour la distributivité.
Souvent, nous allons supprimer l'indice A, donc on va écrire $0, 1, +, \cdot$ sans mentionner A explicitement. On va même écrire parfois A sans mentionner $0, 1, +, \cdot$, mais sachant que $0, 1, +, \cdot$ font partie des données d'un anneau et qu'ils sont fixés. Nous allons aussi supprimer $\cdot$ parfois et écrire ab pour $a \cdot b$. On convient également que la multiplication doit toujours être éxécutée avant l'addition : $a + b \cdot c = a + (b \cdot c)$.

Lemme 8.2. *Soit* $(A, +, \cdot, 0, 1)$ *un anneau. Alors, pour tous* $a \in A$ *on a* $0 \cdot a = a \cdot 0 = 0$.

Démonstration. $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$, donc, $(A, +, 0)$ étant un groupe, on a $0 = 0 \cdot a$. De la même façon : $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$, donc $0 = a \cdot 0$. □

Exemple 8.3. *D'autres exemples d'anneaux sont :*

- $(\mathbb{Q}, +, \cdot, 0, 1)$ *est un anneau commutatif. En appendice, on verra une construction formelle.*
- $(\mathbb{R}, +, \cdot, 0, 1)$ *est un anneau commutatif. Il est connu des cours d'analyse et d'algèbre linéaire. En appendice, on verra une construction formelle.*
- $(\mathrm{Mat}_{2\times 2}(\mathbb{R}), +, \circ, \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right))$ *est un anneau non commutatif (*$\circ$ *désigne le produit matriciel).*

Définition-Lemme 8.4. *Soit* $(A, +, \cdot, 0, 1)$ *un anneau. Un élément* $u \in A$ *est appelé* unité *s'il existe* $v \in A$ *tel que* $uv = vu = 1$. *Une unité est donc un élément inversible dans le monoïde* $(A, \cdot, 1)$.
L'ensemble des unités de A *est noté* $A^\times$. $(A^\times, \cdot, 1)$ *est un groupe (abélien si l'anneau est commutatif). Il s'appelle* groupe des unités de A.

Démonstration. L'associativité et l'existence d'élément neutre proviennent du fait que $(A, \cdot, 1)$ est un monoïde. L'existence d'inverse est la propriété définissant l'ensemble $A^\times$. □

Proposition 8.5. $\mathbb{Z}^\times = \{-1, 1\}$.

Démonstration. L'équation $a \cdot b = 1$ n'admet que les solutions $(a = 1, b = 1)$ et $(a = -1, b = -1)$ dans $\mathbb{Z}$. Donc 1 et -1 sont les seules unités de $\mathbb{Z}$. □

La construction de $\mathbb{Q}$ est fait en appendice. Notre connaissance de $\mathbb{Q}$ nous permet déjà d'affirmer $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$, car toute fraction non nulle $\frac{a}{b}$ a $\frac{b}{a}$ comme inverse.

Anneaux intègres

Proposition 8.6. *Pour tous $a, b \in \mathbb{Z}$ tels que $ab = 0$, on a $a = 0$ ou $b = 0$.*

Démonstration. Si $a \in \mathbb{N}$ et $b \in \mathbb{N}$, c'est la proposition 6.11. Si $a \in \mathbb{N}$ et $b \notin \mathbb{N}$, on a $0 = -1 \cdot 0 = -1 \cdot a \cdot b = a \cdot (-b)$, donc $a = 0$ ou $-b = 0$, donc $a = 0$ ou $b = 0$. Les deux autres cas sont similaires. □

Définition 8.7. *Soit $(A, +, \cdot, 0, 1)$ un anneau. On dit que A est un* anneau intègre *si pour tous $a, b \in A$ tels que $ab = 0$, on a $a = 0$ ou $b = 0$.*
Un élément $a \in A$ tel qu'il existe $b \in A \setminus \{0\}$ avec $ab = 0$ ou $ba = 0$ est appelé diviseur de zéro. *(Donc un anneau est intègre s'il n'existe pas de diviseur de zéro sauf 0.)*

Donc, $(\mathbb{Z}, +, \cdot, 0, 1)$ est un anneau intègre.

Proposition 8.8. *Soit $(A, +, \cdot, 0, 1)$ un anneau intègre. Alors, on peut simplifier des produits comme suit : Pour tous $a, b, c \in A$ avec $a \neq 0$ tels que $ab = ac$ ou $ba = ca$ on a $b = c$.*
En particulier, cette règle est valable dans $\mathbb{Z}$.

Démonstration. Si $ab = ac$, alors $a(b - c) = 0$. Comme A est intègre nous obtenons $a = 0$ ou $b - c = 0$. Le premier cas est exclu, donc $b - c = 0$, donc $b = c$. Un argument similaire marche aussi pour $ba = ca$. □

Corps

Définition 8.9. *Soit $(A, +, \cdot, 0, 1)$ un anneau (commutatif). On l'appelle* corps (commutatif) *si*

- *tout $0 \neq a \in A$ est une unité pour la multiplication (c'est-à-dire, $A^\times = A \setminus \{0\}$) et*
- $0 \neq 1$.

Exemple 8.10.

- *$(\mathbb{Q}, +, \cdot, 0, 1)$ est un corps commutatif.*
- *$(\mathbb{R}, +, \cdot, 0, 1)$ est un corps commutatif.*
- *$(\mathbb{Z}, +, \cdot, 0, 1)$ n'est pas un corps car il existe $n \in \mathbb{Z} \setminus \{0\}$ qui n'est pas une unité, par exemple $n = 2$.*

On définira plus loin une famille de corps très importante : les corps finis.

Lemme 8.11. *Soit $(A, +, \cdot, 0, 1)$ un corps. Alors, A est un anneau intègre.*

Démonstration. Exercice. □

Appendice : Les entiers relatifs

Dans cette section, nous montrons comment construire $\mathbb{Z}$ à partir de $\mathbb{N}$. On n'aura pas le temps de faire cette section en cours, mais on fera quelques exercices.

Construction de $\mathbb{Z}$

D'abord on écrira $\mathcal{Z}$ pour notre construction des entiers relatifs (pour souligner que c'est une construction d'un nouvel objet) ; après la construction, on utilisera la notation habituelle $\mathbb{Z}$ et on calculera avec $\mathbb{Z}$ comme chacun le connaît.
La construction est basée sur la relation d'équivalence suivante.

Lemme 8.12. *La relation binaire sur $\mathbb{N} \times \mathbb{N}$ définie par*

$$(a, b) \sim (c, d) \quad \Leftrightarrow \quad a + d = b + c$$

est une relation d'équivalence.

Démonstration. La preuve est un exercice. La transitivité utilise des propriétés des entiers naturels établies dans la section 6. □

Les classes d'équivalences sont précisément les couples (a, b) ayant la même différence (qui peut être négative !) : donc,

$$\overline{a - b} := \overline{(a, b)} = \{(c, d) \in \mathbb{N} \times \mathbb{N} \mid c - d = a - b\}.$$

On peut donc prendre les classes d'équivalence pour cette relation d'équivalence comme une définition de $\mathbb{Z}$ si on arrive à définir l'addition et la multiplication « habituelles ». On s'occupe d'abord de l'addition.

Proposition 8.13. *Soit $\mathcal{Z}$ l'ensemble quotient de $\mathbb{N}$ par la relation d'équivalence définie dans le lemme 8.12.*

(a) L'application

$$+_{\mathcal{Z}} : \mathcal{Z} \times \mathcal{Z} \to \mathcal{Z}, \quad \overline{(a, b)} +_{\mathcal{Z}} \overline{(c, d)} := \overline{(a + c, b + d)}$$

est bien définie. La définition peut être écrite comme $\overline{a - b} +_{\mathcal{Z}} \overline{c - d} = \overline{(a + c) - (b + d)}$.

(b) Posons $0_{\mathcal{Z}} := \overline{(0, 0)} = \overline{0 - 0}$. Alors, $(\mathcal{Z}, +_{\mathcal{Z}}, 0_{\mathcal{Z}})$ est un groupe abélien et l'inverse de $\overline{a - b} = \overline{(a, b)}$ est $\overline{b - a} = \overline{(b, a)}$; il est aussi noté $-\overline{a - b} = -\overline{(a, b)}$.

(c) L'application

$$i : \mathbb{N} \to \mathcal{Z}, \quad n \mapsto \overline{(n, 0)} = \overline{n - 0}$$

est injective et satisfait $i(a + b) = i(a) +_{\mathcal{Z}} i(b)$ pour tous $a, b \in \mathbb{N}$.

(d) $\overline{a - b} = \overline{(a, b)} \in i(\mathbb{N})$ si et seulement si $a \geq b$.

Démonstration. Exercice. □

Lemme 8.14. *Pour tout $\overline{a - b} = \overline{(a, b)} \in \mathcal{Z} \backslash i(\mathbb{N})$ on a $-\overline{a - b} = \overline{(b, a)} \in i(\mathbb{N})$ et $\overline{(a, b)} = \overline{(0, b - a)}$.*

Démonstration. On a $a < b$, donc $\overline{(b, a)} \in \mathcal{Z}$. Le reste est clair. □

La multiplication des entiers relatifs

Nous allons maintenant définir une multiplication sur notre « modèle » des entiers relatifs.

Proposition 8.15. *(a) L'application*

$$\cdot_{\mathcal{Z}} : \mathcal{Z} \times \mathcal{Z} \to \mathcal{Z}, \quad \overline{(a,b)} \cdot_{\mathcal{Z}} \overline{(c,d)} := \overline{(ac+bd, ad+bc)}$$

est bien définie. On peut l'écrire comme

$$\overline{a-b} \ \cdot_{\mathcal{Z}} \ \overline{c-d} = \overline{(ac+bd)-(ad+bc)}.$$

(b) Posons $1_{\mathcal{Z}} := \overline{(1,0)} = \overline{1-0}$*. Alors,* $(\mathcal{Z}, \cdot_{\mathcal{Z}}, 1_{\mathcal{Z}})$ *est un monoïde abélien.*

(c) La multiplication est distributive*, c'est-à-dire*

$$(\overline{(a,b)} +_{\mathcal{Z}} \overline{(c,d)}) \cdot_{\mathcal{Z}} \overline{(e,f)} = (\overline{(a,b)} \cdot_{\mathcal{Z}} \overline{(e,f)}) +_{\mathcal{Z}} (\overline{(c,d)} \cdot_{\mathcal{Z}} \overline{(e,f)})$$

pour tous $a, b, c, d, e, f \in \mathbb{N}$.

Démonstration. (a) Il faut donc montrer que la définition de $\cdot_{\mathcal{Z}}$ ne dépend pas du choix des représentants des classes. Soient $(a', b') \in \overline{(a,b)}$ et $(c', d') \in \overline{(c,d)}$. Donc par définition on a

$$a + b' = a' + b \quad \text{et} \quad c + d' = c' + d.$$

En conséquence on obtient

$$ac + b'c = a'c + bc, \quad a'd + bd = ad + b'd, \quad a'c + a'd' = a'c' + a'd, \quad b'c' + b'd = b'c + b'd'.$$

On les aditionne pour obtenir :

$$ac + b'c + a'd + bd + a'c + a'd' + b'c' + b'd = a'c + bc + ad + b'd + a'c' + a'd + b'c + b'd',$$

donc

$$(ac+bd) + (a'd' + b'c)' = (a'c' + b'd') + (ad+bc)$$

et en conséquence

$$\overline{(ac+bd, ad+bc)} = \overline{(a'c'+b'd', a'd'+b'c')}.$$

(b) et (c) Exercice. □

L'ordre naturel sur $\mathbb{Z}$

Nous allons étendre l'ordre naturel à $\mathbb{Z}$ (pour obtenir l'ordre « habituel »).
Rappelons que nous avons défini $\mathbb{Z} = \mathcal{Z}$ comme l'ensemble des classes d'équivalence $\overline{a-b} = \overline{(a,b)} = \{(c,d) \in \mathbb{N} \times \mathbb{N} \mid a + d = b + c\}$.

Définition-Lemme 8.16. *(a) Sur* $\mathcal{Z} = \mathbb{Z}$ *on définit une relation d'ordre totale par*

$$\overline{a-b} \preccurlyeq \overline{c-d} \Leftrightarrow a + d \leq b + c.$$

(b) Sur l'image de $\mathbb{N}$ *par l'application naturelle* $i : \mathbb{N} \to \mathcal{Z}, \quad n \mapsto \overline{n-0}$ *cet ordre est le même que l'ordre de* $\mathbb{N}$.

Démonstration. (b) est claire :

$$\overline{n-0} \preccurlyeq \overline{m-0} \Leftrightarrow n+0 \leq m+0 \Leftrightarrow n \leq m.$$

(a)

Bien défini Supposons $\overline{a-b} = \overline{a'-b'}$ (donc, $a+b' = a'+b$) et $\overline{c-d} = \overline{c'-d'}$ (donc, $c+d' = c'+d$). Nous trouvons les équivalences :

$$\begin{aligned}
\overline{a-b} \preccurlyeq \overline{c-d} &\Leftrightarrow a+d \leq b+c \\
&\Leftrightarrow a+d+b'+d' \leq b+c+b'+d' \\
&\Leftrightarrow (a+b')+d+d' \leq (c+d')+b+b' \\
&\Leftrightarrow (a'+b)+d+d' \leq (c'+d)+b+b' \\
&\Leftrightarrow (a'+d')+(b+d) \leq (b'+c')+(b+d) \\
&\Leftrightarrow a'+d' \leq b'+c' \\
&\Leftrightarrow \overline{a'-b'} \preccurlyeq \overline{c'-d'}
\end{aligned}$$

Donc, la définition ne dépend pas du choix.

Réflexivité $\overline{a-b} \preccurlyeq \overline{a-b} \Leftrightarrow a+b \leq b+a$.

Antisymétrie Si $\overline{a-b} \preccurlyeq \overline{c-d}$ et $\overline{c-d} \preccurlyeq \overline{a-b}$, alors, $a+d \leq b+c$ et $b+c \leq a+d$, alors $a+d = b+c$, donc $\overline{a-b} = \overline{c-d}$.

Transitivité

$$\begin{aligned}
&\overline{a-b} \preccurlyeq \overline{c-d} \text{ et } \overline{c-d} \preccurlyeq \overline{e-f} \\
\Rightarrow &a+d \leq b+c \text{ et } c+f \leq d+e \\
\Rightarrow &a+d+f \leq b+c+f \text{ et } c+f \leq d+e \\
\Rightarrow &a+d+f \leq b+d+e \\
\Rightarrow &a+f \leq b+e \\
\Rightarrow &\overline{a-b} \preccurlyeq \overline{e-f}.
\end{aligned}$$

Totalité Soient $\overline{a-b}, \overline{c-d} \in \mathcal{Z}$. Si $a+d \leq b+c$, alors $\overline{a-b} \preccurlyeq \overline{c-d}$. Si $b+c \leq a+d$, alors $\overline{c-d} \preccurlyeq \overline{a-b}$.

□

Après cette preuve nous allons écrire $\leq$ au lieu de $\preccurlyeq$.

Lemme 8.17. *Soient* $x, y, z \in \mathbb{Z}$ *tel que* $x \leq y$. *Alors :*

(a) $x+z \leq y+z$.

(b) Si $0 \leq z$, *alors* $x \cdot z \leq y \cdot z$.

(c) Si $z \leq 0$, *alors* $y \cdot z \leq x \cdot z$.

Démonstration. Soient $x = \overline{a-b}, y = \overline{c-d}, z = \overline{e-f}$. Nous avons $a+d \leq b+c$.
(a) Il en suit que $(a+e)+(d+f) \leq (c+e)+(b+f)$, donc $\overline{a-b}+\overline{e-f} \leq \overline{c-d}+\overline{e-f}$.
(b) Nous pouvons écrire $z = \overline{n-0}$ avec $n \in \mathbb{N}$. D'abord notons que la formule pour la multiplication dans $\mathcal{Z}$ nous donne $xz = xn = \overline{an-bn}$ et $yz = yn = \overline{cn-dn}$. Il suit de $a+d \leq b+c$ que $an+dn \leq bn+cn$, donc $xz = \overline{an-bn} \leq \overline{cn-dn} = yz$.
(c) Nous pouvons écrire $z = \overline{0-n}$ avec $n \in \mathbb{N}$. La formule pour la multiplication dans $\mathcal{Z}$ donne $xz = x\overline{0-n} = \overline{bn-an}$ et $yz = y\overline{0-n} = \overline{dn-cn}$. Il suit de $a+d \leq b+c$ que $an+dn \leq bn+cn$, donc $yz = \overline{dn-cn} \leq \overline{bn-an} = xz$. □

Dans ce cours, on utilise la notation $\mathbb{Z}$ pour $\mathcal{Z}$ et on écrit $+, \cdot$ au lieu de $+_{\mathcal{Z}}, \cdot_{\mathcal{Z}}$. On utilise aussi les notations habituelles n pour $\overline{n-0} = \overline{(n,0)}$ et $-n$ pour $\overline{0-n} = \overline{(0,n)}$ (pour $n \in \mathbb{N}$).

9 L'anneau des entiers relatifs revisité

Objectifs :

- Maîtriser la division euclidienne ;
- maîtriser les congruences et les règles de calculs ;
- connaître la relation entre congruences modulo n et l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$;
- connaître les corps fini premiers.

Magie de nombres (ou pas de magie ?)

Si vous me donnez un nombre naturel n (en écriture décimale), je peux tout de suite vous dire s'il est divisible par 9 ou pas. Connaissez-vous la règle ?
Si vous me donnez un nombre naturel n (en écriture décimale), je peux tout de suite vous dire s'il est divisible par 11 ou pas. Connaissez-vous la règle ?
Si vous me donnez un nombre naturel n, je peux tout de suite vous dire lequel est le dernier chiffre de 3^n (en écriture décimale). Par exemple, le dernier chiffre de

- 3^{122} est 9 ;
- 3^{2016} est 1. Effectivement, $3^{2016} =$

$$\begin{array}{c}
75240126116825753221233832298262396639265375288188565708651873727659316520817250577669105743539835542441748405719721496784672829847339411482640331635962471604046816\\
68317920253720365847033991812451006924496991280275114801542523320574676575510920120965103435094704248125360088077218296287569723791027663717601564030417643946846999\\
44030238138090035041832236412688350514951695446482758356693560837830476406273763706608052458450549266307606256837091889322882430394266759809550318192384195628388185\\
89032988943800573550586386735767268476811040987375451974296972636264910543967836303011328258824090074981412016036286341392348485617137592641583663340608713413771378\\
66583427443951942313249947957460129933029714613534137616281670580917754549712688716598597201988066254435800084857783928207100791439308841923228159261033339078247768\\
79867720971743083575840364151483414698038397696019015500041156826462929809641888942477175130159471390506095902455254180352118267760139102867 21
\end{array}$$

- (voyez le cours)

La divisibilité dans $\mathbb{Z}$

Soit $a, b \in \mathbb{Z}$. On rappelle que b *divise* a (notation : $b \mid a$) s'il existe $q \in \mathbb{Z}$ tel que $a = bq$.

Lemme 9.1. *La divisibilité dans $\mathbb{Z}$ définit une relation réflexive et transitive qui satisfait aussi :*

(a) pour tous $a, b \in \mathbb{Z} \setminus \{0\}$: $\big((a \mid b \text{ et } b \mid a) \Rightarrow a = b \text{ ou } a = -b\big)$ *;*

(b) pour tous $a, b, c \in \mathbb{Z}$: $\big((a \mid b \text{ et } a \mid c) \Rightarrow a \mid (b + c) \text{ et } a \mid (b - c)\big)$.

Démonstration.

Réflexivité $a \mid a$ parce que $a \cdot 1 = a$.

Transitivité $a \mid b$ et $b \mid c$ impliquent l'existence de $q, r \in \mathbb{Z}$ tels que $b = qa$ et $c = rb$. Donc $c = qra$, donc $a \mid c$.

(a) $a \mid b$ et $b \mid a$ impliquent l'existence de $q, r \in \mathbb{Z}$ tels que $b = qa$ et $a = rb$. Donc $a = rqa$, donc (a étant non nul et $\mathbb{Z}$ intègre) $rq = 1$, et donc $r = \pm 1$ et $q = r$ par la proposition 8.5, d'où le résultat.

(b) $a \mid b$ et $a \mid c$ impliquent l'existence de $q, r \in \mathbb{Z}$ tels que $b = qa$ et $c = ra$. Donc, $b + c = (q + r)a$ et $b - c = (q - r)a$, donc $a \mid (b + c)$ et $a \mid (b - c)$.

□

Division euclidienne

Proposition 9.2 (Division euclidienne)**.** *Soient $x, y \in \mathbb{Z}$ avec $y \geq 1$. Il existe des uniques $q, r \in \mathbb{Z}$ tels que*

$$x = qy + r \text{ et } 0 \leq r \leq y - 1.$$

Démonstration.

Existence Soit $M := \{x - zy \mid z \in \mathbb{Z}\} \cap \mathbb{N}$. C'est un sous-ensemble non-vide de $\mathbb{N}$. Comme $\mathbb{N}$ est bien ordonné, il existe un plus petit élément $r \in M$; il est automatiquement de la forme $r = x - qy$. Si $r \geq y$, alors $r - y = x - (q + 1)y \in M$ est un élément encore plus petit que le plus petit élément. Donc $r < y$.

Unicité Supposons que $x = qy + r = q'y + r'$. Donc,

$$(q - q')y = r' - r.$$

Il en suit $y \mid (r' - r)$. Mais, on a aussi

$$-y < r' - r < y,$$

donc $0 = r' - r$ (car 0 est le seul multiple de y strictement plus grand que $-y$ et strictement plus petit que y), donc $r = r'$ et $q = q'$.

□

Congruences

Définition 9.3. *Soit $n \in \mathbb{N}_{>0}$. Deux entiers relatifs $x, y \in \mathbb{Z}$ sont appelés* congrus modulo n *si* $n \mid (x-y)$.
Notation : $x \equiv y \pmod{n}$ *(ou* $x \equiv y \mod (n)$*).*

Lemme 9.4. *Soient $n \in \mathbb{N}_{>0}$ et $x, y \in \mathbb{Z}$. Les assertions suivantes sont équivalentes :*

(i) $x \equiv y \pmod{n}$.

(ii) Le reste de la division euclidienne de x par n est le même que le reste de la division de y par n.

Démonstration. Soient $x = q_1 n + r_1$ et $y = q_2 n + r_2$ avec $0 \leq r_1 \leq n-1$ et $0 \leq r_2 \leq n-1$.
« (i) $\Rightarrow$ (ii) » : Alors, $n \mid (x-y)$. Comme $n \mid (q_1 - q_2)n$, il suit que n divise $(x-y) - (q_1-q_2)n = r_1 - r_2$, donc $r_1 = r_2$ (même argument qu'en haut : $-n < r_1 - r_2 < n$).
« (ii) $\Rightarrow$ (i) » : Alors, $r_1 = r_2$, donc $x - y = (q_1 - q_2)n$, donc $n \mid (x-y)$, donc $x \equiv y \pmod{n}$. □

Définition-Lemme 9.5. *Soit $n \in \mathbb{N}$. La congruence modulo n définit une relation d'équivalence R_n :*

$$\forall (x,y) \in \mathbb{Z}^2, x R_n y \Leftrightarrow x \equiv y \pmod{n}.$$

L'ensemble quotient $\mathbb{Z}/R_n$ est noté $\mathbb{Z}/n\mathbb{Z}$. On a :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

et

$$\overline{0} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}, \overline{k} = \{\ldots, -2n+k, -n+k, k, n+k, 2n+k, \ldots\}.$$

La classe d'un entier k compris entre 0 et $n-1$ est le sous-ensemble de $\mathbb{Z}$ formé des entiers relatifs dont le reste dans la division euclidienne par n est égal à k.

Démonstration. Exercice. □

Anneaux quotients

Lemme 9.6. *Soient $n \in \mathbb{N}$ et $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ tels que*

$$x_1 \equiv y_1 \pmod{n} \quad \textit{et} \quad x_2 \equiv y_2 \pmod{n}.$$

Alors,

$$x_1 + x_2 \equiv y_1 + y_2 \pmod{n} \quad \textit{et} \quad x_1 \cdot x_2 \equiv y_1 \cdot y_2 \pmod{n}.$$

Démonstration. Nous avons $n \mid (x_1 - y_1)$ et $n \mid (x_2 - y_2)$.
Pour la première assertion nous en concluons $n \mid ((x_1 - y_1) + (x_2 - y_2))$, donc $n \mid ((x_1 + x_2) - (y_1 + y_2))$, donc $x_1 + x_2 \equiv y_1 + y_2 \pmod{n}$.
Pour la deuxième assertion, il suit que $n \mid (x_1 - y_1)x_2$ et $n \mid (x_2 - y_2)y_1$, donc $n \mid ((x_1 - y_1)x_2 + (x_2 - y_2)y_1)$, donc $n \mid (x_1 x_2 - y_1 y_2)$, donc $x_1 \cdot x_2 \equiv y_1 \cdot y_2 \pmod{n}$. □

On peut maintenant donner l'explication du calcul du dernier chiffre de 3^n pour $n \in \mathbb{N}$. Faire la division euclidienne de n par 4 : $n = 4q + r$ avec $0 \leq r \leq 3$. Alors :

$$3^n = 3^{4q+r} = (3^4)^q \cdot 3^r = 81^q \cdot 3^r \equiv 1^q \cdot 3^r = 3^r \pmod{10}.$$

Donc, le magicien n'a besoin que de faire la division euclidienne par 4 (pour ça il suffit de la faire pour les 2 derniers chiffres de n (trouvez la raison vous-mêmes !)) et de connaître (le dernier chiffre de) 3^r pour $r = 0, 1, 2, 3$.

Définition-Lemme 9.7. *Soit $n \in \mathbb{N}$. Nous définissons*

$$+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad (\overline{x}, \overline{y}) \mapsto \overline{x} + \overline{y} := \overline{x + y}$$

et

$$\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad (\overline{x}, \overline{y}) \mapsto \overline{x} \cdot \overline{y} := \overline{x \cdot y}.$$

Alors, $(\mathbb{Z}/n\mathbb{Z}, +, \cdot, \overline{0}, \overline{1})$ est un anneau commutatif.

Démonstration. Exercice. Utiliser le lemme 9.6 pour démontrer que $+$ et $\cdot$ sont bien définis (indépendants des choix de représentants) et le fait que $(\mathbb{Z}, +, \cdot, 0, 1)$ est un anneau. □

Nous allons souvent noter les classes de $\mathbb{Z}/n\mathbb{Z}$ sans écrire les « barres ». Également, on notera l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot, \overline{0}, \overline{1})$ plus court comme $\mathbb{Z}/n\mathbb{Z}$.

Exemple 9.8. *(a) Voici les tables d'addition et de multiplication de $\mathbb{Z}/2\mathbb{Z}$.*

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

(b) Voici les tables d'addition et de multiplication de $\mathbb{Z}/3\mathbb{Z}$.

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

(c) Voici les tables d'addition et de multiplication de $\mathbb{Z}/4\mathbb{Z}$.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Plus grand diviseur commun (pgcd)

Définition 9.9. *Soient $d \in \mathbb{N}$ et $x, y \in \mathbb{Z}$. On appelle d* plus grand commun diviseur de x, y *(notation : $d = \mathrm{pgcd}(x, y)$) si*

- *$d \mid x$ et $d \mid y$ et*

- *pour tout* $e \in \mathbb{N}$ *on a* $((e \mid x$ *et* $e \mid y) \Rightarrow e \mid d)$.

Proposition 9.10. *Soient* $x, y \in \mathbb{Z}$ *pas tous les deux* 0.

(a) Un plus grand commun diviseur de x *et* y *existe et il est unique.*

(b) Identité de Bézout : *Il existe* $a, b \in \mathbb{Z}$ *tels que* $\mathrm{pgcd}(x, y) = ax + by$.

Démonstration. Soit $M := \{ax + by \mid a, b \in \mathbb{Z}\}$ et $M^+ := M \cap \mathbb{N}_{>0}$. Comme M^+ est un sous-ensemble non vide de $\mathbb{N}$, il possède un plus petit élément d (par le fait que $\mathbb{N}$ est bien ordonné).
Par définition il existe $a, b \in \mathbb{Z}$ tel que $d = ax + by$. Nous allons démontrer que d est un plus grand commun diviseur de x, y.
D'abord on montre $d \mid m$ pour tout $m \in M$ (comme $x, y \in M$, on obtient alors automatiquement $d \mid x$ et $d \mid y$). Soit $m = ux + vy$. On fait la division euclidienne par d :

$$m = qd + r \text{ avec } 0 \leq r \leq d - 1.$$

Alors,

$$r = m - qd = ux + vy - q(ax + by) = (u - qa)x + (v - qb)y,$$

donc $r = 0$ car si $1 \leq r$, alors $r \in M^+$ entraînerait que r est strictement plus petit que le plus petit élément de M^+, une contradiction.
Soit $e \in \mathbb{N}$ tel que $e \mid x$ et $e \mid y$. Donc, $e \mid (ax + by)$, donc $e \mid d$. Nous avons terminé la preuve que d est un plus grand commun diviseur.
L'unicité est claire : Si $d, e \in \mathbb{N}$ sont des plus grands communs diviseurs tous les deux, alors $d \mid e$ et $e \mid d$, et e et d sont tous les deux dans $\mathbb{N}_{>0}$, donc $d = e$. □

Le pgcd et l'identité de Bézout peuvent être calculés (et leur existence peut être démontrée) par l'algorithme d'Euclide (voir Exercices) que nous décrivons maintenant (et que vous avez dû voir à l'école).
Soient $r_0 \geq r_1$ deux entiers positifs. Nous allons calculer leur pgcd ainsi que l'identité de Bézout, par le processus récursif suivant :

Si $r_1 \geq 1$, calculer le reste r_2 de la div. de r_0 par r_1	$r_0 = q_1 r_1 + r_2$;
Si $r_2 \geq 1$, calculer le reste r_3 de la div. de r_1 par r_2	$r_1 = q_2 r_2 + r_3$;
$\vdots$	$\vdots$
Si $r_n \geq 1$, calculer le reste r_{n+1} de la div. de r_{n-1} par r_n	$r_{n-1} = q_n r_n + r_{n+1}$;
Si $r_{n+1} = 0$, on a terminé.	$r_n = \mathrm{pgcd}(r_0, r_1)$

Nous démontrons ci-dessous que r_n est en effet égal à $\mathrm{pgcd}(r_0, r_1)$. D'abord on vérifie que r_n divise r_0 et r_1 :

r_n divise r_{n-1}.
$\Rightarrow$ r_n divise $r_{n-2} = q_{n-1} r_{n-1} + r_n$.
$\Rightarrow$ r_n divise $r_{n-3} = q_{n-2} r_{n-2} + r_{n-1}$.
$\vdots$
$\Rightarrow$ r_n divise $r_1 = q_2 r_2 + r_3$.
$\Rightarrow$ r_n divise $r_0 = q_1 r_1 + r_2$.

Exemple 9.11. $r_0 = 99$ *et* $r_1 = 21$.

Calculer le reste $r_2 = 15$ *de la div. de* 99 *par* 21	$99 = 4 \cdot 21 + 15$ *;*
Calculer le reste $r_3 = 6$ *de la div. de* 21 *par* 15	$21 = 1 \cdot 15 + 6$ *;*
Calculer le reste $r_4 = 3$ *de la div. de* 15 *par* 6	$15 = 2 \cdot 6 + 3$ *;*
Le reste de la div. de 6 *par* 3 *est* 0	$6 = 2 \cdot 3$ *;*
	$3 = \mathrm{pgcd}(99, 21)$

On obtient l'identité de Bézout en utilisant les égalités dans la colonne à droite, commençant par le bas :

$$\begin{aligned} 3 &= 15 - 2 \cdot 6 \\ &= 15 - 2 \cdot (21 - 1 \cdot 15) = -2 \cdot 21 + 3 \cdot 15 \\ &= -2 \cdot 21 + 3 \cdot (99 - 4 \cdot 21) = 3 \cdot 99 - 14 \cdot 21. \end{aligned}$$

Le calcul de l'identité de Bézout dans l'exemple est un peu *ad hoc*. On va le remplacer par une formulation générale et plus élégante. On utilisera les matrices de taille 2×2 qu'on suppose connues du cours d'algèbre linéaire.

Soient $r_0 \geq r_1$ deux entiers positifs. Nous allons calculer leur pgcd ainsi que l'identité de Bézout, par le processus récursif suivant :

Si $r_1 \geq 1$, reste r_2 de la div. de r_0 par r_1	$A_1 := \left(\begin{smallmatrix} -q_1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} r_2 \\ r_1 \end{smallmatrix}\right) = A_1 \left(\begin{smallmatrix} r_1 \\ r_0 \end{smallmatrix}\right)$
Si $r_2 \geq 1$, reste r_3 de la div. de r_1 par r_2	$A_2 := \left(\begin{smallmatrix} -q_2 & 1 \\ 1 & 0 \end{smallmatrix}\right) \cdot A_1$	$\left(\begin{smallmatrix} r_3 \\ r_2 \end{smallmatrix}\right) = A_2 \left(\begin{smallmatrix} r_1 \\ r_0 \end{smallmatrix}\right)$
$\vdots$	$\vdots$	$\vdots$
Si $r_n \geq 1$, reste r_{n+1} de la div. de r_{n-1} par r_n	$A_n := \left(\begin{smallmatrix} -q_n & 1 \\ 1 & 0 \end{smallmatrix}\right) \cdot A_{n-1}$	$\left(\begin{smallmatrix} r_{n+1} \\ r_n \end{smallmatrix}\right) = A_n \left(\begin{smallmatrix} r_1 \\ r_0 \end{smallmatrix}\right)$
Si $r_{n+1} = 0$, on a terminé.	$r_n = \mathrm{pgcd}(r_0, r_1)$	

Soit $A_{n-1} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Alors, l'égalité $\left(\begin{smallmatrix} r_n \\ r_{n-1} \end{smallmatrix}\right) = A_{n-1} \left(\begin{smallmatrix} r_1 \\ r_0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \left(\begin{smallmatrix} r_1 \\ r_0 \end{smallmatrix}\right)$ nous donne

$$r_n = ar_1 + br_0,$$

l'identité de Bézout récherchée. Comme on sait que r_n divise r_0 et r_1, on obtient aussi une preuve que r_n est en effet le pgcd de r_0 et r_1 : tout diviseur de r_0 et r_1 doit diviser r_n.

Exemple 9.12. *On reprend l'exemple* $r_0 = 99$ *et* $r_1 = 21$.

Reste $r_2 = 15$ *de la div. de* 99 *par* 21	$A_1 = \left(\begin{smallmatrix} -4 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ *;*
Reste $r_3 = 6$ *de la div. de* 21 *par* 15	$A_2 = \left(\begin{smallmatrix} -1 & 1 \\ 1 & 0 \end{smallmatrix}\right) \cdot A_1 = \left(\begin{smallmatrix} 5 & -1 \\ -4 & 1 \end{smallmatrix}\right)$ *;*
Reste $r_4 = 3$ *de la div. de* 15 *par* 6	$A_3 = \left(\begin{smallmatrix} -2 & 1 \\ 1 & 0 \end{smallmatrix}\right) \cdot A_2 = \left(\begin{smallmatrix} -14 & 3 \\ 5 & -1 \end{smallmatrix}\right)$ *;*
Le reste de la div. de 6 *par* 3 *est* 0	
	$3 = \mathrm{pgcd}(99, 21)$

Les coefficients de l'identité de Bézout sont les coefficients de la première rangée de la matrice A_3 *:*

$$3 = -14 \cdot 21 + 3 \cdot 99.$$

Définition 9.13. *Soient* $m \in \mathbb{N}$ *et* $x, y \in \mathbb{Z}$*. On appelle* m *le* plus petit commun multiple de x, y *(notation :* $m = \mathrm{ppcm}(x, y)$*) si*

- $x \mid m$ *et* $y \mid m$ *et*
- *pour tout* $n \in \mathbb{N}$ *on a* $((x \mid n \text{ et } y \mid n) \Rightarrow m \mid n)$.

Proposition 9.14. *Soient $x, y \in \mathbb{Z}$ pas tous les deux 0.*

(a) Un plus petit commun multiple de x et y existe et il est unique.

(b) On a l'identité $xy = \mathrm{signe}(xy) \cdot \mathrm{ppcm}(x, y) \cdot \mathrm{pgcd}(x, y)$.

Démonstration. Exercice. □

Corps finis

Lemme 9.15. *Soit $n \in \mathbb{N}_{>1}$. Soit $\omega \in \mathbb{Z}/n\mathbb{Z}$. Les assertions suivantes sont équivalented :*

(i) $\exists\, x \in \omega : \mathrm{pgcd}(x, n) = 1$

(ii) $\forall\, x \in \omega : \mathrm{pgcd}(x, n) = 1$

(iii) ω est inversible dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot, \overline{0}, \overline{1})$.

En particulier, is $x \in \mathbb{Z}$ est tel que $\mathrm{pgcd}(x, n) = 1 = ax + bn$ avec $a, b \in \mathbb{Z}$ (l'identité de Bézout), alors, la classe $\overline{a}$ est l'inverse multiplicatif de la classe $\overline{x}$.

Démonstration. (i) ⇒ (ii) : Soit $x \in \omega$. Si $\mathrm{pgcd}(x, n) = 1$, il existe une relation de Béuout $1 = ax + bn$. Soit $y \in \omega$. Alors, $y = x + rn$ et donc $1 = ay + (b - r)n$. On en conclut $\mathrm{pgcd}(y, n) = 1$.
(ii) ⇒ (iii) : Soit $\mathrm{pgcd}(x, n) = 1 = ax + bn$ une relation de Bézout. Elle donne $1 \equiv ax \mod n$.
(iii) ⇒ (i) : Soit $x \in \omega$ and $\overline{a}$ l'inverse de ω. Donc $\overline{1} = \omega \cdot \overline{a} = \overline{x} \cdot \overline{a}$, d'où $1 = ax + bn$ pour un $b \in \mathbb{Z}$. Cela implique $\mathrm{pgcd}(x, n) = 1$. □

Corollaire 9.16. *Soit $n \in \mathbb{N}_{>1}$. Alors, le groupe des unités de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot, \overline{0}, \overline{1})$ est*

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{x} \mid x \in \mathbb{Z}, \mathrm{pgcd}(x, n) = 1\}.$$

Démonstration. Dans le lemme 9.15 nous avons vu que toutes les classes $\overline{x}$ pour $x \in \mathbb{Z}$ tel que $\mathrm{pgcd}(x, n) = 1$ sont des unités.
Si $x = py$ et $n = pm$ avec $1 < p \leq n$, alors nous avons $\overline{m} \neq \overline{0}$ et

$$\overline{x} \cdot \overline{m} = \overline{y} \cdot \overline{p} \cdot \overline{m} = \overline{y} \cdot \overline{pm} = \overline{y} \cdot \overline{0} = \overline{0},$$

donc $\overline{x}$ ne peut pas être une unité, car s'il l'était : $\overline{1} = \overline{zx}$, alors

$$\overline{m} = \overline{1}\overline{m} = \overline{zxm} = \overline{z}\overline{0} = \overline{0},$$

une contradiction. □

Corollaire 9.17. *Soit $n \in \mathbb{N}_{>1}$. Les assertions suivantes sont équivalentes :*

(i) $(\mathbb{Z}/n\mathbb{Z}, +, \cdot, \overline{0}, \overline{1})$ est un corps commutatif de cardinal n.

(ii) n est un nombre premier.

Si p est un nombre premier, on note $\mathbb{F}_p := (\mathbb{Z}/p\mathbb{Z}, +, \cdot, \overline{0}, \overline{1})$, et on l'appelle le corps fini de cardinal p.

Démonstration. « (i) $\Rightarrow$ (ii) » : Supposons que n n'est pas un nombre premier, donc $n = ab$ avec $1 < a, b < n$. Alors par le corollaire 9.16 $\overline{a} \neq \overline{0}$ n'est pas une unité de $\mathbb{Z}/n\mathbb{Z}$, donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas un corps.
« (ii) $\Rightarrow$ (i) » : Si n est un nombre premier, tous les $a \in \mathbb{Z}$ tels que $1 \leq a \leq n-1$ satisfont $\mathrm{pgcd}(a, n) = 1$, donc toutes les classes $\overline{1}, \overline{2}, \ldots, \overline{n-1}$ sont inversibles. Donc, la seule classe qui n'est pas inversible est $\overline{0}$ et $\mathbb{Z}/n\mathbb{Z}$ est un corps. □

Appendice : Unique factorisation en nombres premiers

Dans cet appendice, nous donnons une caractérisation alternative des nombres premiers. Au cours d'algèbre, cette caractérisation va nous servir de modèle pour une généralisation des nombres premiers dans des anneaux plus généraux que $\mathbb{Z}$. Ici, nous en avons besoin pour démontrer le fait que tout nombre naturel s'écrit de façon (essentiellement) unique comme produit de nombres premiers.
Nous rappelons que nous avons déjà démontré le théorème d'Euclide que le nombre de nombres premiers est infini (théorème 1.5).

Lemme 9.18. *Soit $p \in \mathbb{N}_{>1}$. Les assertion suivantes sont équivalentes :*

(i) p est un nombre premier.

(ii) Pour tout $a, b \in \mathbb{Z}$ on a : si p divise le produit ab, alors p divise a ou p divise b.

Démonstration. « (i) $\Rightarrow$ (ii) » : Soit p un nombre premier tel que $p \nmid a$. On veut montrer $p \mid b$.
Comme $p \nmid a$ et les seuls diviseurs positifs de p sont 1 et p, on a $\mathrm{pgcd}(a, p) = 1$ et l'identité de Bézout $1 = rp + sa$ pour certains $r, s \in \mathbb{Z}$. Puisque p divise ab, il divise aussi sab et brp, donc $p \mid (sab + brp)$, mais

$$sab + brp = (1 - rp)b + brp = b - brp + brp = b,$$

donc $p \mid b$.
« (ii) $\Rightarrow$ (i) » : Supposons que l'assertion (i) est fausse, c'est-à-dire que p n'est pas un nombre premier. Alors $p = ab$ avec $1 < a, b < p$ et $a, b \in \mathbb{N}$. Donc $p \mid p = ab$, mais $p \nmid a$ et $p \nmid b$, donc l'assertion (ii) est fausse. □

Corollaire 9.19. *Soient $p \in \mathbb{N}_{>1}$ un nombre premier, $s \in \mathbb{N}_{\geq 2}$ et $q_1, \ldots, q_s \in \mathbb{Z}$ tels que $p \mid q_1 q_2 \ldots q_s$. Alors il existe $i \in \{1, \ldots, s\}$ tel que $p \mid q_i$.*

Démonstration. Par récurrence pour $s \geq 2$. L'initialisation $s = 2$ est le contenu du lemme 9.18. Supposons que l'assertion est vraie pour un s. Nous allons la démontrer pour $s + 1$. Donc, supposons que $p \mid q_1 q_2 \ldots q_s q_{s+1}$. On le réécrit comme $p \mid ab$ avec $a = q_1 q_2 \ldots q_s$ et $b = q_{s+1}$. Par le lemme 9.18 il suit que $p \mid a$ ou $p \mid b$. Dans le dernier cas $p \mid q_{s+1}$. Dans le premier cas par l'hérédité nous obtenons $p \mid q_i$ pour un $i \in \{1, \ldots, s\}$, donc, l'assertion est vraie pour $s + 1$. □

Lemme 9.20. *Soit $n \in \mathbb{N}_{\geq 2}$. Alors, il existe un nombre premier p qui divise n.*

Démonstration. Nous avons déjà fait cet argument dans la preuve de l'infinitude des nombres premiers. On le refait ici :

$$M := \{m \in \mathbb{N}_{\geq 2} \mid m \text{ divise } n\}.$$

C'est un sous-ensemble de $\mathbb{N}$ qui n'est pas vide (car $n \in M$ comme $n \mid n$). Donc, comme $\mathbb{N}$ est bien ordonné, il existe un plus petit élément $p \in M$. Soit $t \in \mathbb{N}_{>1}$ un diviseur de p. Alors, par le lemme 9.1 (a) on a $t \mid n$, donc $t \in M$. Comme $t \leq p$ et p est le plus petit élément de M, il en suit que $t = p$, donc p est un nombre premier. □

Théorème 9.21 (Théorème fondamental de la théorie élémentaire des nombres)**.** *Tout nombre naturel $n \geq 1$ s'écrit comme produit fini de nombres premiers de façon unique à l'ordre près. ($n = 1$ correspond au produit vide.)*
Plus précisement on a pour tout $n \geq 2$:

(a) Il existe $r \in \mathbb{N}$ et $p_1, \ldots, p_r \in \mathbb{P}$ (des nombres premiers) tel que $n = p_1 p_2 \ldots p_r$.

(b) Si $s \in \mathbb{N}$ et $q_1, \ldots, q_s \in \mathbb{P}$ tels que $n = q_1 q_2 \ldots q_s$, alors $r = s$ et il existe une bijection $\sigma : \{1, \ldots, r\} \to \{1, \ldots, r\}$ telle que pour tout $i \in \{1, \ldots, r\}$ on a $q_i = p_{\sigma(i)}$.

Démonstration.
(a) Soit

$$M := \{n \in \mathbb{N}_{\geq 2} \mid n \text{ n'est pas un produit fini de nombres premiers }\}.$$

C'est un sous-ensemble de $\mathbb{N}$. Supposons qu'il n'est pas vide, alors il possède un plus petit élément m. Par le lemme 9.20 il existe un nombre premier p qui divise m. Comme p est un produit de nombres premiers (le produit avec le seul facteur p), on a $p \notin M$, donc $p < m$, donc $2 \leq \frac{m}{p} < m$, donc $\frac{m}{p} \notin M$. Donc $\frac{m}{p}$ est un produit d'éléments premiers, donc $m = p\frac{m}{p}$ l'est aussi. Donc $m \notin M$. Contradiction. Donc M est vide.
(b) Nous démontrons le résultat par récurrence pour $n \geq 1$. Pour $n = 1$ le résultat est clair. Supposons que nous avons déjà démontré le résultat pour tout nombre naturel positif strictement plus petit que n. Montrons-le pour n.
Nous avons donc

$$p_1 p_2 \ldots p_r = n = q_1 q_2 \ldots q_s.$$

Comme $p_1 \mid n$, il suit du corollaire 9.19 qu'il existe un $j \in \{1, \ldots, s\}$ tel que $p_1 \mid q_j$. Comme q_j et p_1 sont des nombres premiers, on a $p_1 = q_j$. En conséquence, nous obtenons

$$p_2 \ldots p_r = \frac{n}{p_1} = q_1 q_2 \ldots q_{j-1} q_{j+1} \ldots q_s.$$

Comme $1 \leq \frac{n}{p_1} < n$, par hérédité $r - 1 = s - 1$ (donc $r = s$) et il existe une bijection $\sigma : \{1, \ldots, j-1, j+1, \ldots, r\} \to \{2, 3, \ldots, r\}$ telle que $q_i = p_{\sigma(i)}$ pour tout $i \in \{1, \ldots, j-1, j+1, \ldots, r\}$. Nous prolongeons $\sigma : \{1, \ldots, r\} \to \{1, \ldots, r\}$ en posant $\sigma(j) = 1$. Evidemment, σ est une bijection. □

Appendice : Les nombres rationnels

Cette appendice ne sera pas traitée dans le cours, mais il y aura quelques exercices pour vous familiariser avec le contenu. Ici, nous montrons comment les nombres rationnels sont **construits** à partir des entiers relatifs. Donc vous pouvez vous convaincre à l'aide de cette section que les nombres rationnels ont aussi une fondation solide.

Construction des nombres rationnels

Nous avons construit l'anneau $(\mathbb{Z}, +, \cdot, 0, 1)$. Maintenant, nous allons l'utiliser pour une construction des nombres rationnels.
Nous allons définir les fractions comme des classes d'équivalence pour tenir compte du fait que le numérateur et le dénominateur d'une fraction ne sont pas uniques (on peut les multiplier par n'importe quel entier non nul : $\frac{a}{b} = \frac{ac}{bc}$).

Définition-Lemme 9.22. *Sur $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ on définit une relation*

$$(a, x) \sim (b, y) \Leftrightarrow ay = bx.$$

C'est une relation d'équivalence.
La classe de (a, x) est formée de tous les (b, y) tel que $ay = bx$, ce qui justifie la notation $\frac{a}{x}$ pour la classe $\overline{(a, x)}$.
L'ensemble quotient est noté $\mathbb{Q}$, l'ensemble des nombres rationnels.

Démonstration. Exercice. □

Proposition 9.23. *Soit $\mathbb{Q}$ l'ensemble quotient du lemme 9.22.*

(a) Les deux applications

$$+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}, \quad \frac{a}{x} + \frac{b}{y} := \frac{ay + bx}{xy}$$

et

$$\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}, \quad \frac{a}{x} \cdot \frac{b}{y} := \frac{ab}{xy}$$

sont bien définies, c'est-à-dire que leurs définitions ne dépendent pas des choix des représentants (a, x) et (b, y) des classes $\frac{a}{x}$ et $\frac{b}{y}$.

(b) $(\mathbb{Q}, +, \cdot, \frac{0}{1}, \frac{1}{1})$ est un corps.

(c) L'application

$$\iota : \mathbb{Z} \to \mathbb{Q}, \quad n \mapsto \frac{n}{1}$$

est injective et on a $\iota(n + m) = \iota(n) + \iota(m)$ et $\iota(n \cdot m) = \iota(n) \cdot \iota(m)$.

Démonstration. Exercice. □

L'ordre naturel sur $\mathbb{Q}$

Définition-Lemme 9.24. *(a) Sur $\mathbb{Q}$ on définit une relation d'ordre totale par*

$$\frac{a}{b} \preccurlyeq \frac{c}{d} :\Leftrightarrow ad \leq bc$$

pour $b, d \in \mathbb{N}_{>0}$.

(b) Sur l'image de $\mathbb{Z}$ par l'application naturelle $\iota : \mathbb{Z} \to \mathbb{Q}, \quad n \mapsto \frac{n}{1}$ cet ordre est le même que l'ordre de $\mathbb{Z}$.

Démonstration. La démonstration n'est pas difficile et peut être faite comme exercice. □

À partir de maintenant nous allons écrire $\leq$ au lieu de $\preccurlyeq$.

Lemme 9.25. *Soient $x, y, z \in \mathbb{Q}$ tel que $x \leq y$. Alors :*

(a) $x + z \leq y + z$.

(b) Si $0 \leq z$, *alors* $x \cdot z \leq y \cdot z$.

(c) Si $z \leq 0$, *alors* $y \cdot z \leq x \cdot z$.

Démonstration. La démonstration n'est pas difficile et peut être faite comme exercice. □

La valeur absolue de $\mathbb{Q}$

Définition 9.26. *Pour $r \in \mathbb{Q}$ nous définissons* la valeur absolue de r *par*

$$|x| := \begin{cases} r & \text{si } 0 \leq r, \\ -r & \text{si } r \leq 0. \end{cases}$$

Proposition 9.27. *Pour $r, s \in \mathbb{Q}$ les assertions suivantes sont vraies :*

(a) $|r| \geq 0$ *et* $r = 0 \Leftrightarrow |r| = 0$.

(b) $|r \cdot s| = |r| \cdot |s|$ *(multiplicativité).*

(c) $|r + s| \leq |r| + |s|$ *(inégalité triangulaire).*

(d) Il existe $n \in \mathbb{N}$ tel que $|n| > 1$ (cette propriété « triviale » dit que la valeur propre est « archimédienne » ; il existe aussi des valeurs absolues qui ne sont pas archimédiennes).

Démonstration. (a) La seule chose à montrer est la suivante : Soit $r \leq 0$. Alors, $-1 \cdot 0 = 0 \leq -1 \cdot r = -r$, donc $0 \leq -r$.
(b) Clair.
(c) Nous avons $r \leq |r|$ et $s \leq |s|$ (on le vérifie directement). Donc $r + s \leq |r| + |s|$. De la même manière on conclut de $-r \leq |r|$ et $-s \leq |s|$ que $-(r + s) \leq |r| + |s|$. Les deux ensemble nous donnent : $|r + s| \leq |r| + |s|$.
(d) $|2| = 2 > 1$. □

Corollaire 9.28 (Deuxième inégalité triangulaire)**.** *Pour tout $r, s \in \mathbb{Q}$ on a :*

$$\big||r| - |s|\big| \leq |r + s| \leq |r| + |s|.$$

Démonstration. Nous avons $|r| = |r + s - s| \leq |r + s| + |s|$, donc $|r| - |s| \leq |r + s|$. De la même manière nous avons $|s| - |r| \leq |r + s|$, donc $\big||r| - |s|\big| \leq |r + s|$. □

Les nombres réels

Les nombres réels sont un objet étudié dans vos cours d'Analyse. Pour être complet, nous rajoutons encore une esquisse de la construction des nombres réels à partir des nombres rationnels.
Dans vos cours d'analyse, vous avez défini des suites de Cauchy (dans $\mathbb{Q}$ avec convergence pour la valeur absolue définie ci-dessus). Soit $\mathcal{C}$ l'ensemble de toutes les suites de Cauchy. Soit $\mathcal{N}$ le sous-ensemble de $\mathcal{C}$ des suites de Cauchy qui tendent vers 0.
Sur $\mathcal{C}$ on définit la relation d'équivalence

$$(a_n)_{n\in\mathbb{N}} \sim (b_n)_{n\in\mathbb{N}} :\Leftrightarrow (a_n - b_n)_{n\in\mathbb{N}} \in \mathcal{N}.$$

L'ensemble quotient de $\mathcal{C}$ modulo cette relation d'équivalence est l'ensemble des nombres réels. Les nombres rationnels s'y plongent via l'application qui envoie $x \in \mathbb{Q}$ sur la suite constante $a_n := x$ pour tout $n \in \mathbb{N}$. On additionne et multiplie deux classes (nombres réels) en additionnant ou multipliant des suites de Cauchy qui représentent ces classes terme par terme.

Chapitre III

Plus sur les groupes

10 Sous-groupes et ordres

Objectifs :

- Apprendre et maîtriser la définition de sous-groupes ;
- apprendre et maîtriser les groupes cycliques ;
- apprendre et maîtriser la génération de sous-groupes ;
- Apprendre et maîtriser l'ordre d'un élément dans un groupe ;
- savoir démontrer des propriétés simples.

Nous rappelons d'abord les groupes que nous connaissons déjà :

- $(\mathbb{Z}, +, 0)$, $(\mathbb{Z}^\times, \cdot, 1) = (\{-1, +1\}, \cdot, 1)$.
- $(\mathbb{Q}, +, 0)$, $(\mathbb{Q}^\times, \cdot, 1) = (\mathbb{Q} \setminus \{0\}, \cdot, 1)$.
- $(\mathbb{Z}/n\mathbb{Z}, +, \overline{0})$, $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot, \overline{1})$.
- $(S_n, \circ, (1))$, le groupe symétrique.

Comme la définition l'exige, il s'agit d'un ensemble avec une « loi de groupe » qui est associative, possède un élément neutre et telle que chaque élément a un inverse. Si la loi de groupe est écrite « multiplicativement », on note l'inverse de a par a^{-1} ; si la loi est notée « additivement », on écrit $-a$ pour l'inverse de a.
Dans cette section nous allons étudier des sous-groupes. L'idée est simple : un sous-groupe d'un groupe est un sous-ensemble qui est « respecté » par la loi de groupe. Nous allons préciser ceci dans la définition suivante.
Regardons un exemple : Considérons $\mathbb{Z}$ comme groupe pour l'addition et deux sous-ensembles :

- $P := \{n \in \mathbb{Z} \mid n \text{ est pair }\}$,
- $I := \{n \in \mathbb{Z} \mid n \text{ est impair }\}$.

Bien que les deux sous-ensembles aient l'air très similaires, ils ne le sont pas du tout du point de vue suivant :
Si $a, b \in P$, alors $a + b \in P$. Mais : si $a, b \in I$, alors $a + b \notin I$. Nous voyons que la loi de groupe respecte P mais pas I.
D'ailleurs, l'élément neutre appartient à $P : 0 \in P$, mais pas à $I : 0 \notin I$. Par contre pour P et I on a que l'inverse de tout élément de l'ensemble y appartient aussi : si $a \in P$, alors $-a \in P$; si $a \in I$, alors $-a \in I$.

Définition 10.1. *Soit $(G, \star, e)$ un groupe et $H \subseteq G$ un sous-ensemble. H est appelé* sous-groupe de *G (notation $H \leq G$) si*

- $e \in H$,
- *pour tout $a, b \in H$ on a $a \star b \in H$ (donc, $\star$ donne une application $H \times H \to H$), et*
- *pour tout $a \in H$, l'inverse $a^{-1} \in H$.*

Exemple 10.2.

- *P est un sous-groupe de $(\mathbb{Z}, +, 0)$, mais I ne l'est pas.*
- *Pour tout $n \in \mathbb{Z}$ l'ensemble de tous les multiples de n est aussi un sous-groupe de $(\mathbb{Z}, +, 0)$.*
  En fait, tout sous-groupe de $\mathbb{Z}$ est de cette forme.
- *Soit $(G, \star, e)$ un groupe. L'ensemble $\{e\}$ est un sous-groupe de G.*
- *Soit $(G, \star, e)$ un groupe. G est un sous-groupe de G.*
- *$\{-1, +1\} \subseteq \mathbb{Q}$ est un sous-groupe de $(\mathbb{Q}^\times, \cdot, 1)$, mais pas un sous-groupe de $(\mathbb{Q}, +, 0)$.*
- *Soit $S_3 = (S_3, \circ, (1))$ le groupe symétrique en $\{1, 2, 3\}$. Nous considérons l'ensemble $H := \{(1\ \ 2\ \ 3), (1\ \ 3\ \ 2), (1)\}$; c'est un sous-groupe, mais l'ensemble $\{(1\ \ 2), (1\ \ 3), (2\ \ 3), (1)\}$ ne l'est pas.*

Dans ce cours et dans les cours à suivre nous définissons souvent des « sous-objets d'objets » (autre exemple : sous-espace vectoriel) ; à chaque fois on exige que le sous-objet soit un objet du même type : un sous-espace vectoriel est un espace vectoriel ; ici : un sous-groupe est un groupe :

Lemme 10.3. *Soit $(G, \star, e)$ un groupe et $H \subseteq G$ un sous-ensemble. Alors, les assertions suivantes sont équivalentes.*

(i) *H est un sous-groupe de G.*

(ii) *On a $\star(H \times H) \subseteq H$, $e \in H$ et $(H, \star, e)$ est un groupe.*

Démonstration. « (i) $\Rightarrow$ (ii) » : C'est clair : l'associativité provient de celle de G ainsi que le fait que e est l'élément neutre. En plus, e appartient à H par définition et les inverses de H y appartiennent aussi par définition.
« (ii) $\Rightarrow$ (i) » : Il suffit de montrer que pour $a \in H$, son inverse a^{-1} (dans le groupe G) appartient à H. Comme $(H, \star, e)$ est un groupe, l'élément a possède un inverse $b \in H$. L'unicité de l'inverse (lemme 7.5) montre que $b = a^{-1}$. □

Le lemme prochain donne un critère qui permet souvent de raccourcir la preuve qu'un sous-ensemble donné est un sous-groupe.

Lemme 10.4 (Critère pour sous-groupes)**.** *Soit $(G, \star, e)$ un groupe et $H \subseteq G$ un sous-ensemble non-vide. Alors les assertions suivantes sont équivalentes :*

(i) $H \leq G$ *(H est un sous-groupe de G).*

(ii) Pour tout $a, b \in H$ *on a* $a \star b^{-1} \in H$.

Démonstration. « (i) $\Rightarrow$ (ii) » : Soient $a, b \in H$. Comme H est un sous-groupe, on a $b^{-1} \in H$ et donc $a \star b^{-1} \in H$.
« (ii) $\Rightarrow$ (i) » : Comme H est non-vide, il y existe un élément $a \in H$. L'hypothèse nous donne $a \star a^{-1} \in H$, donc $e \in H$. Pour tout $b \in H$ on obtient $e \star b^{-1} = b^{-1} \in H$. Soient $a, b \in H$, donc $a \star (b^{-1})^{-1} = a \star b \in H$. Nous avons vérifié la définition et concluons que H est un sous-groupe de G. □

Exemple 10.5. *Tout élément du groupe $(\mathbb{Z}, +, 0)$ s'écrit en utilisant seulement 1 (et son inverse -1) ; par exemple $0 = 1 + (-1)$, $5 = 1 + 1 + 1 + 1 + 1$ et $-5 = -1 - 1 - 1 - 1 - 1$.*
On en déduit qu'un sous-groupe de $H \leq \mathbb{Z}$ qui contient 1 est automatiquement égal à $\mathbb{Z}$.

Définition 10.6. *Soit $(G, \star, e)$ un groupe. G est appelé* cyclique *s'il existe $g \in G$ tel que tout élément de G est de la forme g^n pour $n \in \mathbb{Z}$ où*

$$g^n = \begin{cases} e & \text{si } n = 0, \\ \underbrace{g \star g \star \cdots \star g}_{n\text{-fois}} & \text{si } n > 0, \\ \underbrace{g^{-1} \star g^{-1} \star \cdots \star g^{-1}}_{|n|\text{-fois}} & \text{si } n < 0. \end{cases}$$

Exemple 10.7.
- *Le groupe $(\mathbb{Z}, +, 0)$ est cyclique.*
- *Pour tout $n \in \mathbb{N}$ le groupe $(\mathbb{Z}/n\mathbb{Z}, +, \overline{0})$ est cyclique.*

Lemme 10.8. *Tout groupe cyclique est abélien.*

Démonstration. C'est évident : $g^n \star g^m = g^{n+m} = g^{m+n} = g^m \star g^n$ pour tout $n, m \in \mathbb{Z}$. □

Définition 10.9. *Soient $(G, \star, e)$ un groupe et $M \subseteq G$ un sous-ensemble. On dit que G est* engendré *par M (et que M est un* ensemble de générateurs*) si le seul sous-groupe de G qui contient M est G lui-même.*

Lemme 10.10. *Soit $(G, \star, e)$ un groupe. Les assertions suivantes sont équivalentes :*

(i) G est cyclique.

(ii) Il existe un ensemble de générateurs M de G de cardinal 1.

Démonstration. « (i) $\Rightarrow$ (ii) » : Soit G cyclique avec élément « spécial » g. Si $H \leq G$ est un sous-groupe qui contient g, il contient automatiquement tous les éléments de G, donc $H = G$. Ceci montre que $M = \{g\}$ est un ensemble de générateurs.
« (ii) $\Rightarrow$ (i) » : Soit $M = \{g\}$ un ensemble de générateurs d'un seul élément. On pose $H := \{g^n \mid n \in \mathbb{Z}\}$. C'est un sous-groupe de G à cause du critère du lemme 10.4 : $g^n \star (g^m)^{-1} = g^{n-m} \in H$. Comme $g \in H$, l'hypothèse implique $H = G$, donc, G est cyclique. □

Nous allons maintenant généraliser ceci à un ensemble de générateurs de cardinal quelconque.

Définition-Lemme 10.11. *Soient $(G, \star, e)$ un groupe et $M \subseteq G$ un sous-ensemble. On pose*

$$\langle M \rangle := \{x_1^{\epsilon_1} \star x_2^{\epsilon_2} \star \cdots \star x_n^{\epsilon_n} \mid n \in \mathbb{N}, x_i \in M, \epsilon_i \in \{-1, 1\}\}.$$

En mots : $\langle M \rangle$ est le sous-ensemble de G de ceux éléments de G qui s'écrivent comme produit d'éléments dans M et leurs inverses. Noter que le cas $n = 0$ (produit vide) correspond à l'élément neutre e. Alors $\langle M \rangle$ est un sous-groupe de G et tout sous-groupe de G qui contient M, contient aussi $\langle M \rangle$. En particulier, $\langle M \rangle$ est engendré par M.
Pour cette raison on l'appelle aussi le sous-groupe de G engendré par M.

Démonstration. Montrons d'abord que $\langle M \rangle$ est un sous-groupe de G en utilisant le lemme 10.4. Soient $x_1^{\epsilon_1} \star x_2^{\epsilon_2} \star \cdots \star x_n^{\epsilon_n}$ et $y_1^{\delta_1} \star y_2^{\delta_2} \star \cdots \star y_m^{\delta_m}$ deux éléments de $\langle M \rangle$. Alors

$$x_1^{\epsilon_1} \star x_2^{\epsilon_2} \star \cdots \star x_n^{\epsilon_n} \star y_m^{-\delta_m} \star \cdots \star y_2^{-\delta_2} \star y_1^{-\delta_1}$$

appartient aussi à $\langle M \rangle$. Donc $\langle M \rangle$ est un sous-groupe de G.
Il est clair que tout sous-groupe H de G qui contient les éléments de M aussi contient leurs inverses et tous les produits finis. Donc $\langle M \rangle \subseteq H$. Cela implique que $\langle M \rangle$ est engendré par M. □

Si G est cyclique de générateur g, alors $G = \langle g \rangle = \langle \{g\} \rangle$. Noter que si G n'est pas abélien, $x_1 \star x_2 \star x_1 \neq x_1^2 \star x_2$ en général.
Nous allons maintenant donner une construction plus abstraite du sous-groupe engendré par un ensemble M. Pour cela nous devons d'abord démontrer que l'intersection de sous-groupe est un sous-groupe.

Lemme 10.12. *Soient $(G, \star, e)$ un groupe, I un ensemble « d'indices » (par ex. $I = \{1, 2, \ldots, n\}$) et pour tout $i \in I$ soit H_i un sous-groupe de G. On pose $H := \bigcap_{i \in I} H_i$, l'intersection de tous les H_i. Alors, H est un sous-groupe de G.*

Démonstration.

- Commes les H_i sont des sous-groupes, on a $e \in H_i$ pour tout $i \in I$. Donc, $e \in \bigcap_{i \in I} H_i = H$.
- Soient $a, b \in \bigcap_{i \in I} H_i = H$. Donc, pour tout $i \in I$ on a $a, b \in H_i$. Comme H_i est un sous-groupe de G, on a $a \star b^{-1} \in H_i$, pour tout $i \in I$. Donc, $a \star b^{-1} \in \bigcap_{i \in I} H_i = H$. Par le lemme 10.4 H est un sous-groupe de G.

□

Proposition 10.13. *Soit $(G, \star, e)$ un groupe et $M \subseteq G$ un sous-ensemble. Alors*

$$\langle M \rangle = \bigcap_{H \leq G, M \subseteq H} H,$$

l'intersection de tous les sous-groupes H de G qui contiennent M.

Démonstration. Comme $\langle M \rangle$ est un groupe et contient M, on a que $\langle M \rangle$ fait partie des sous-groupes dans l'intersection. Alors nous avons l'inclusion « $\supseteq$ ».
Si H est un sous-groupe de G qui contient M, alors $\langle M \rangle \subseteq H$, donc nous avons l'inclusion « $\subseteq$ ». □

Exemple 10.14. *(a) Le groupe symétrique S_n (avec $n \in \mathbb{N}_{\geq 2}$) est engendré par les transpositions (voir exercices).*

(b) Le group $(M_{2\times 2}(\mathbb{Z}), +, \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right))$ est engendré par les matrices $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

Définition 10.15. *Soit $(G, \cdot, 1)$ un groupe. Pour un élément $g \in G$ on définit* l'ordre *de g (notation : $\mathrm{ord}(g)$) comme le plus petit entier positif $n > 0$ tel que $g^n = 1$, l'élément neutre (si un tel n n'existe pas, alors on dit que $\mathrm{ord}(g) = \infty$).*

Exemple 10.16.

- *Dans tout groupe, l'ordre de l'élément neutre est 1 et c'est le seul élément d'ordre 1.*

  Raison : $g = g^1 = 1$.

- *Les ordres des éléments du groupe symétrique S_3 sont les suivants :*

$$\mathrm{ord}\big((1)\big) = 1, \ \ \mathrm{ord}\big((1\ 2)\big) = 2, \ \ \mathrm{ord}\big((1\ 3)\big) = 2,$$
$$\mathrm{ord}\big((2\ 3)\big) = 2, \ \ \mathrm{ord}\big((1\ 2\ 3)\big) = 3, \ \ \mathrm{ord}\big((1\ 3\ 2)\big) = 3.$$

- *Les ordres des éléments de $(\mathbb{Z}/6\mathbb{Z}, +, \overline{0})$ sont les suivants :*

$$\mathrm{ord}(\overline{0}) = 1, \ \ \mathrm{ord}(\overline{1}) = 6, \ \ \mathrm{ord}(\overline{2}) = 3, \ \ \mathrm{ord}(\overline{3}) = 2, \ \ \mathrm{ord}(\overline{4}) = 3, \ \ \mathrm{ord}(\overline{5}) = 6.$$

  Donc $\mathbb{Z}/6\mathbb{Z}$ est un groupe cyclique qui peut être engendré par $\overline{1}$ ou $\overline{5} = \overline{-1}$.

- *Dans $(\mathbb{Z}, +, 0)$, l'ordre de tout $0 \neq m \in \mathbb{Z}$ est infini (car $nm \neq 0$ pour tout $n \in \mathbb{N}_{>0}$).*

Lemme 10.17. *Soient G un groupe et $g \in G$.*

(a) On suppose $n = \mathrm{ord}(g) < \infty$. Soit $m \in \mathbb{Z}$. Alors, $g^m = 1$ si et seulement si $n \mid m$.

(b) Soit $m \in \mathbb{N}$ tel que $m < \mathrm{ord}(g)$. Alors, les éléments $1, g, g^2, \ldots, g^m$ sont deux à deux distincts.

Démonstration. (a) Supposons d'abord $m = nq$ avec $q \in \mathbb{Z}$. Alors, $g^m = g^{nq} = (g^n)^q = 1^q = 1$.
Soit maintenant $m \in \mathbb{Z}$ tel que $g^m = 1$. La division euclidienne nous donne $m = q\,\mathrm{ord}(g) + r$ avec $0 \leq r \leq \mathrm{ord}(g) - 1$. Donc $1 = g^m = (g^{\mathrm{ord}(g)})^q \cdot g^r = 1^q \cdot g^r = g^r$. La seule possibilité est $r = 0$ car sinon l'existence de r contradirait la définition de l'ordre.
(b) On suppose que l'assertion est fausse. Alors, on a $g^a = g^b$ avec $0 \leq a < b \leq m$, ce qui donne $g^{b-a} = 1$, une contradiction car $0 < b - a \leq m < \mathrm{ord}(g)$. □

Proposition 10.18. *Soient G un groupe et $g \in G$. Alors,*

$$\mathrm{ord}(g) = \#\langle g \rangle.$$

En mots : l'ordre du sous-groupe engendré par g est égal à l'ordre de g.

Démonstration. Supposons d'abord que $\mathrm{ord}(g)$ est infini. Alors pour tout $m \in \mathbb{N}$ les éléments $1, g, g^2, \ldots, g^m$ sont distincts par le lemme 10.17 (b), donc $\langle g \rangle$ est un groupe de cardinal infini.
Supposons maintenant $\mathrm{ord}(g) = n < \infty$. Alors les n éléments $1, g, g^2, \ldots, g^{n-1} \in \langle g \rangle$ sont distincts, encore par le lemme 10.17 (b). On montre que $\langle g \rangle = \{g^m \mid m \in \mathbb{Z}\} = \{1, g, g^2, \ldots, g^{n-1}\}$. Soit donc $g^m \in \langle g \rangle$. On utilise la division euclidienne pour écrire $m = qn + r$ avec $0 \leq r < n$. Nous avons $g^m = g^{qn+r} = (g^n)^q \cdot g^r = 1^q \cdot g^r = g^r$. Cela montre l'inclusion « $\subseteq$ ». L'autre inclusion est triviale. □

Corollaire 10.19. *Soit G un groupe fini. Alors les assertions suivantes sont équivalentes :*

(i) *G est cyclique.*

(ii) *$\exists\, g \in G : \mathrm{ord}(g) = \#G$.*

Démonstration. Cela provient directement de la proposition 10.18. □

11 Le théorème de Lagrange et son application aux ordres

Objectifs :

- Apprendre et maîtriser les classes d'un groupe suivant un sous-groupe ;
- connaître la définition de l'indice d'un sous-groupe ;
- connaître et savoir démontrer le théorème de Lagrange ;
- connaître et savoir démontrer le 'petit Fermat de la théorie des groupes' à partir du théorème de Lagrange ;
- savoir démontrer des propriétés simples.

A partir de cette section on utilisera la convention suivante : si on dit « soit G un groupe », on l'écrit multiplicativement $g \cdot h = gh$ et on note 1 son élément neutre.

Définition-Lemme 11.1. *Soit G un groupe et $H \leq G$ un sous-groupe. La relation définie par*

$$g_1 \sim_H g_2 \quad :\Leftrightarrow \quad g_1^{-1} \cdot g_2 \in H$$

est une relation d'équivalence.
Les classes d'équivalence sont de la forme

$$gH = \{g \cdot h \mid h \in H\}$$

et elles s'appellent classes à gauche de G suivant H. *L'ensemble de ces classes est noté G/H.*
Donc, on a

- $G = \bigsqcup_{gH \in G/H} gH$,
- $g_1H \cap g_2H = \begin{cases} \emptyset & \text{si } g_1^{-1}g_2 \notin H, \\ g_1H & \text{si } g_1^{-1}g_2 \in H. \end{cases}$

Un élément $g_2 \in g_1H$ est appelé un représentant. *On a alors $g_1H = g_2H$.*

Démonstration. La vérification que c'est une relation d'équivalence est un exercice. Le reste est une conséquence valable pour toutes les relations d'équivalence (voir la proposition 5.16). □

Exemple 11.2. *$\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes à gauche du groupe $\mathbb{Z}$ (pour l'addition) suivant le sous-groupe $n\mathbb{Z}$.*
En effet, dans la définition-lemme 9.5 nous avons défini la relation d'équivalence

$$x \sim_{R_n} y \Leftrightarrow x \equiv y \pmod{n}.$$

Nous avons

$$x \equiv y \pmod{n} \Leftrightarrow x - y \in n\mathbb{Z}.$$

Donc la relation d'équivalence définie dans 9.5 est la même que celle de 11.1.

Définition-Lemme 11.3. *Soit G un groupe et $H \leq G$ un sous-groupe.*

(a) De la même manière que dans la définition-lemme 11.1 on définit les classes à droite de G suivant H*, en utilisant la relation d'équivalence*

$$g_1 \sim_H g_2 \quad :\Leftrightarrow \quad g_1 \cdot g_2^{-1} \in H.$$

Les classes à droites sont de la forme

$$Hg = \{h \cdot g \mid h \in H\}$$

et l'ensemble de toutes ces classes est noté $H\backslash G$. On a

- $G = \bigsqcup_{Hg \in H\backslash G} Hg$,
- $Hg_1 \cap Hg_2 = \begin{cases} \emptyset & \text{si } g_1g_2^{-1} \notin H, \\ Hg_1 & \text{si } g_1g_2^{-1} \in H. \end{cases}$

(b) L'application

$$\phi : G/H \to H\backslash G, \quad gH \mapsto Hg^{-1}$$

est bijective.

Démonstration. C'est clair ! (Noter pour (b) que $Hg^{-1} = (gH)^{-1}$ parce que $H^{-1} = H$.) □

Lemme 11.4. *Soient G un groupe et $H \leq G$ un sous-groupe. Pour tout $g_1, g_2 \in G$ l'application*

$$g_1H \longrightarrow g_2H, \quad g_1h \mapsto (g_2g_1^{-1})g_1h = g_2h$$

est bijective. Donc $\#H = \#gH$ pour tout $g \in G$ (les deux peuvent être infinis).

Démonstration. La surjectivité est évidente. Regardons donc l'injectivité : $g_2h_1 = g_2h_2$ implique $g_2^{-1}g_2h_1 = g_2^{-1}g_2h_2$, donc $h_1 = h_2$. □

Définition 11.5. *Soient G un groupe et $H \leq G$ un sous-groupe.* L'indice de H dans G *est défini par*

$$(G : H) := \#G/H = \#H\backslash G$$

(il peut être infini).

Théorème 11.6 (Lagrange)**.** *Soient G un groupe et $H \leq G$ un sous-groupe. Alors :*

$$\#G = (G : H) \cdot \#H.$$

Démonstration. C'est une conséquence immédiate de la réunion disjointe $G = \bigsqcup_{gH \in G/H} gH$ et le fait $\#H = \#gH$ pour tout $g \in G$ par le lemme 11.4.
Plus précisement, on va distinguer les cas $\#G = \infty$ et $\#G < \infty$. Si $\#G = \infty$, il suit de la réunion disjointe que $\#H = \#gH$ est infini ou que $(G : H)$ est infini. Dans les deux cas, le produit $(G : H) \cdot \#H$ est infini. Si $\#G < \infty$, il est clair que $(G : H)$ et $\#H$ sont tous les deux finis. La formule est maintenant claire. □

Corollaire 11.7. *Soient G un groupe fini et $H \leq G$ un sous-groupe. Alors, $\#H$ divise $\#G$ et l'indice $(G : H)$ divise $\#G$.*

Démonstration. Cela suit directement du théorème de Lagrange 11.6 $\#G = (G : H) \cdot \#H$ car l'indice est entier. □

Exemple 11.8. *(a) Si H est un sous-groupe de S_3, sa cardinalité ne peut pas être 4 ou 5 car les seuls diviseurs de $\#S_3 = 6$ sont $1, 2, 3, 6$. Il existe des sous-groupes de cardinal $1, 2, 3, 6$ (trouvez les vous-mêmes !).*

(b) Si $H \lneq S_4$ est un sous-groupe, sa cardinalité est inférieure ou égale à 12 et elle ne peut pas être $5, 7, 9, 10, 11$ car les seuls diviseurs de $\#S_4 = 24$ sont $1, 2, 3, 4, 6, 8, 12$.

(c) Le groupe S_5 de cardinal 120 ne possède pas de sous-groupe de cardinal 15 (c'est un exercice).

Noter : $15 \mid 120$. Donc en général, pour un diviseur n de $\#G$ il n'existe pas de sous-groupe de G de cardinal n.

Corollaire 11.9. *Soient G un groupe fini et $g \in G$. Alors $\mathrm{ord}(g) \mid \#G$.*
En mots : l'ordre de tout élément divise l'ordre du groupe.

Démonstration. Par le corollaire 11.7 du théorème de Lagrange et la proposition 10.18 on a $\mathrm{ord}(g) = \#\langle g\rangle \mid \#G$. □

Corollaire 11.10 (« Petit théorème de Fermat de la théorie des groupes »)**.** *Soit G un groupe fini. Alors, pour tout $g \in G$ on a $g^{\#G} = 1$.*

Démonstration. Cela suit directement du corollaire 11.9 et du lemme 10.17 (a). □

Corollaire 11.11. *Soit G un groupe fini tel que son cardinal $\#G$ est un nombre premier. Alors G est cyclique.*

Démonstration. Soit $p = \#G$, un nombre premier par hypothèse. Soit $g \in G$ différent de 1. Comme $\mathrm{ord}(g)$ divise p (par le corollaire 11.9) et $\mathrm{ord}(g) \neq 1$, alors $\mathrm{ord}(g) = p$, donc G est cyclique par le corollaire 10.19. □

12 Homomorphismes

Objectifs :

- Apprendre et maîtriser la définition de homomorphisme de groupes, de l'image et du noyau ;
- apprendre et maîtriser les propriétés fondamentales des homomorphismes de groupes, de leurs images et de leurs noyaux ;
- connaître et savoir démontrer la classification des groupes cycliques ;
- asvoir appliquer les résultats à la classification des groupes de très petit cardinal ;
- savoir démontrer des propriétés simples.

L'idée générale (valable pour groupes, anneaux, espaces vectoriels, etc.) est la suivante : Un (homo)-morphisme est une application qui respecte toutes les structures.

Exemple 12.1.

- *Soient $c : \mathbb{Z} \to \mathbb{Z}$ l'application définie par $n \mapsto 2n$ et $d : \mathbb{Z} \to \mathbb{Z}$ l'application définie par $n \mapsto 2n + 1$. Nous analysons leurs propriétés :*
  - *c et d sont injectives.*
  - *$c(n + m) = 2(n + m) = 2n + 2m = c(n) + c(m)$ pour tout $n, m \in \mathbb{Z}$.*
  - *$c(0) = 0$.*
  - *$d(n + m) = 2(n + m) + 1 \neq (2n + 1) + (2m + 1) = d(n) + d(m)$ pour $n, m \in \mathbb{Z}$.*
  - *$d(0) = 1$.*
  - *L'image de c est l'ensemble P, donc un sous-groupe de $(\mathbb{Z}, +, 0)$.*
  - *L'image de d est l'ensemble I, donc elle n'est pas un sous-groupe de $(\mathbb{Z}, +, 0)$.*

  Première conclusion : L'application c « respecte » la loi de groupe de $(\mathbb{Z}, +, 0)$ et elle envoie l'élément neutre 0 sur l'élément neutre. L'application d n'a aucune de ces deux propriétés.

- *Soit $\iota : \mathbb{Z} \to \mathbb{Q}$ l'injection donnée par $n \mapsto \frac{n}{1}$.*
  - *$\iota(n + m) = \frac{n+m}{1} = \frac{n}{1} + \frac{m}{1} = \iota(n) + \iota(m)$ pour tout $n, m \in \mathbb{Z}$.*
  - *$\iota(0) = \frac{0}{1}$.*
  - *$\iota(n \cdot m) = \frac{nm}{1} = \frac{n}{1} \cdot \frac{m}{1} = \iota(n) \cdot \iota(m)$ pour tout $n, m \in \mathbb{Z}$.*
  - *$\iota(1) = \frac{1}{1}$.*

Première conclusion : L'application ι « transforme » la loi de groupe de $(\mathbb{Z}, +, 0)$ en la loi de groupe de $(\mathbb{Q}, +, 0)$ et elle envoie l'élément neutre 0 pour la première loi sur l'élément neutre 0 pour la deuxième loi.

De plus, l'application ι « transforme » la loi de groupe de $(\mathbb{Z}^\times, \cdot, 1) = (\{-1; 1\}, \cdot, 1)$ en la loi de groupe de $(\mathbb{Q}^\times, \cdot, 1)$ et elle envoie l'élément neutre 1 pour la première loi sur l'élément neutre 1 pour la deuxième loi.

- *Soit $\exp : \mathbb{R} \to \mathbb{R}_{>0}$ l'exponentielle de vos cours d'analyse.*
  - *$\exp$ est une bijection.*
  - *$\exp(x + y) = \exp(x) \cdot \exp(y)$ pour tout $x, y \in \mathbb{R}$.*
  - *$\exp(0) = 1$.*

  Première conclusion : L'application $\exp$ « transforme » la loi de groupe de $(\mathbb{R}, +, 0)$ en la loi de groupe de $(\mathbb{R}_{>0}, \cdot, 1)$ et elle envoie l'élément neutre 0 de $(\mathbb{R}, +, 0)$ sur l'élément neutre 1 de $(\mathbb{R}_{>0}, \cdot, 1)$.

Ces propriétés nous mènent naturellement à la définition suivante :

Définition 12.2. *Soient $(G, \star, e)$ et $(H, \circ, \epsilon)$ deux groupes. Une application*

$$\varphi : G \to H$$

est appelée homomorphisme de groupes *si pour tout $g_1, g_2 \in G$ on a*

$$\varphi(g_1 \star g_2) = \varphi(g_1) \circ \varphi(g_2).$$

Notation : Pour être très précis, on écrit les homomorphismes de groupes comme

$$(G, \star, e) \to (H, \circ, \epsilon).$$

Normalement, on est moins précis, et si on écrit : « Soit $\varphi : G \to H$ un homomorphisme de groupes » on sous-entend que les lois de groupes et les éléments neutres sont fixés et connus du lecteur.

Exemple 12.3.

- *$c : \mathbb{Z} \to \mathbb{Z}$, donnée par $n \mapsto 2n$, est un homomorphisme de groupes de $(\mathbb{Z}, +, 0)$ dans $(\mathbb{Z}, +, 0)$. Par contre, d n'est pas un homomorphisme de groupes.*
- *$\iota : \mathbb{Z} \to \mathbb{Q}$, donnée par $n \mapsto \frac{n}{1}$ est un homomorphisme de groupes de $(\mathbb{Z}, +, 0)$ dans $(\mathbb{Q}, +, 0)$.*
- *$\exp : \mathbb{R} \to \mathbb{R}_{>0}$ est un homomorphisme de groupes de $(\mathbb{R}, +, 0)$ dans $(\mathbb{R}_{>0}, \cdot, 1)$.*
- *Soit $n \in \mathbb{N}$. On définit :*

  $$\pi : (\mathbb{Z}, +, 0) \to (\mathbb{Z}/n\mathbb{Z}, +, \overline{0}), \quad a \mapsto \overline{a},$$

  l'application qui envoie a sur sa classe modulo n. C'est un homomorphisme de groupes par le lemme 9.6.

- *Soit $(G, \star, e)$ un groupe et $H \leq G$ un sous-groupe. L'inclusion $i : H \to G$ (donnée par $h \mapsto h$) est un homomorphisme de groupes.*

Définition 12.4. *Soient $(G, \star, e)$ et $(H, \circ, \epsilon)$ des groupes et $\varphi : (G, \star, e) \to (H, \circ, \epsilon)$ un homomorphisme de groupes.*

- $\mathrm{im}(\varphi) := \varphi(G) := \{\varphi(g) \mid g \in G\}$ *est appelé* l'image de G par φ.
- *Plus généralement, soit $G' \leq G$ un sous-groupe. $\varphi(G') := \{\varphi(g) \mid g \in G'\}$ est appelé* l'image de G' par φ.
- $\ker(\varphi) := \{g \in G \mid \varphi(g) = \epsilon\}$ *est appelé le* noyau de φ *(en allemand* Kern*, en anglais* kernel*).*

Exemple 12.5. *Le noyau de l'homomorphisme*

$$\pi : (\mathbb{Z}, +, 0) \to (\mathbb{Z}/n\mathbb{Z}, +, \overline{0}), \quad a \mapsto \overline{a}$$

est égal à $\{m \mid n$ divise $m\}$, l'ensemble des multiples de n.

Définition-Lemme 12.6. *Soit $n \in \mathbb{N}_{\geq 1}$ et $(S_n, \circ, (1))$ le groupe symétrique. On définit l'application* signe (ou signature) *par*

$$\mathrm{sgn} : S_n \to \{+1, -1\}, \quad \pi \mapsto \prod_{1 \leq i < j \leq n} \frac{\pi(i) - \pi(j)}{i - j}.$$

C'est un homomorphisme de groupes. Son noyau est noté A_n et appelé le groupe alterné.
Le signe de toute transposition $(i \quad j)$ (avec $i \neq j$) est -1.

Démonstration. Exercice. □

Proposition 12.7 (Propriétés des homomorphismes de groupes)**.** *Soient $(G, \star, e)$ et $(H, *, \epsilon)$ des groupes et $\varphi : (G, \star, e) \to (H, *, \epsilon)$ un homomorphisme de groupes. Alors :*

(a) $\varphi(e) = \epsilon$.

(b) Pour tout $g \in G$ on a : $\varphi(g^{-1}) = \varphi(g)^{-1}$.

(c) Si $G' \leq G$ est un sous-groupe, alors $\varphi(G') \leq H$ est aussi un sous-groupe. En particulier, $\mathrm{im}(\varphi)$ est un sous-groupe de H.

(d) Si $H' \leq H$ est un sous-groupe, alors $\varphi^{-1}(H') \leq G$ est aussi un sous-groupe. (Attention : Ici $\varphi^{-1}(H')$ est l'image réciproque et pas un inverse de l'application !)

(e) Si $\psi : (H, *, \epsilon) \to (I, \otimes, u)$ est un homomorphisme de groupes, alors $\psi \circ \varphi : (G, \star, e) \to (I, \otimes, u)$ est aussi un homomorphisme de groupes.

(f) $\ker(\varphi) \leq G$ *est un sous-groupe.*

Démonstration. (a) On a $\varphi(e) = \varphi(e \star e) = \varphi(e) * \varphi(e)$, donc $\epsilon = \varphi(e) * (\varphi(e))^{-1} = \varphi(e) * \varphi(e) * (\varphi(e))^{-1} = \varphi(e)$.
(b) Par (a) on a $\epsilon = \varphi(e) = \varphi(g \star g^{-1}) = \varphi(g) * \varphi(g^{-1})$. donc, $(\varphi(g))^{-1} = (\varphi(g))^{-1} * \epsilon = (\varphi(g))^{-1} * \varphi(g) * \varphi(g^{-1}) = \varphi(g^{-1})$.
(c) Les éléments dans l'image $\varphi(G')$ sont de la forme $\varphi(g)$ pour $g \in G'$. Soient $\varphi(g_1), \varphi(g_2)$ avec $g_1, g_2 \in G'$ deux éléments de $\varphi(G')$. Comme $g_1 \star g_2^{-1} \in G'$ (car G' est un sous-groupe de G), on conclut que $\varphi(g_1 \star g_2^{-1}) = \varphi(g_1) * \varphi(g_2^{-1}) = \varphi(g_1) * \varphi(g_2)^{-1}$ appartient aussi à $\varphi(G')$ où on utilise (b) pour la dernière égalité. Par le lemme 10.4 nous obtenons donc que $\varphi(G')$ est un sous-groupe de H.
(d) Soit $g_1, g_2 \in \varphi^{-1}(H')$, donc, par définition, cela veut dire $\varphi(g_i) \in H'$ pour $i = 1, 2$. Comme H' est un sous-groupe de H, $\varphi(g_1) * \varphi(g_2)^{-1} \in H'$, donc $\varphi(g_1 \star g_2^{-1}) \in H'$.
(e) Soient $g_1, g_2 \in G$. Alors, $\psi(\varphi(g_1 \star g_2)) = \psi(\varphi(g_1) * \varphi(g_2)) = \psi(\varphi(g_1)) \otimes \psi(\varphi(g_2))$.
(f) Soient $g_1, g_2 \in \ker(\varphi)$. Par définition cela veut dire que $\varphi(g_1) = \epsilon = \varphi(g_2)$. Par (a) et (b) nous avons $\varphi(g_1 \star g_2^{-1}) = \varphi(g_1) * \varphi(g_2)^{-1} = \epsilon * \epsilon^{-1} = \epsilon$, donc $g_1 \star g_2^{-1} \in \ker(\varphi)$. Par le lemme 10.4 nous obtenons donc que $\ker(\varphi)$ est un sous-groupe de G.
On peut aussi remarquer que $\ker(\varphi)$ est l'image réciproque par φ de l'ensemble $\{\epsilon\}$, qui est un sous-groupe de H, et utiliser (d). □

L'utilité du noyau est de caractériser si l'homomorphisme est injectif (comme en algèbre linéaire).

Proposition 12.8. *Soient $(G, \star, e)$ et $(H, \circ, \epsilon)$ des groupes et $\varphi : (G, \star, e) \to (H, \circ, \epsilon)$ un homomorphisme de groupes.*

(a) Les assertions suivantes sont équivalentes :

- *(i)* *φ est surjectif.*
- *(ii)* $H = \mathrm{im}(\varphi)$.

(b) Les assertions suivantes sont équivalentes :

- *(i)* *φ est injectif.*
- *(ii)* $\ker(\varphi) = \{e\}$.

Démonstration. (a) C'est par définition ! On le mentionne ici uniquement à cause de la similarité avec (b).
(b) « (i) $\Rightarrow$ (ii) » : Soit $g \in \ker(\varphi)$. Alors, $\varphi(g) = \epsilon = \varphi(e)$, donc $g = e$ par l'injectivité de φ.
« (ii) $\Rightarrow$ (i) » : Soient $g_1, g_2 \in G$ tels que $\varphi(g_1) = \varphi(g_2)$. Donc $\epsilon = \varphi(g_2)^{-1} \circ \varphi(g_1) = \varphi(g_2^{-1}) \circ \varphi(g_1) = \varphi(g_2^{-1} \star g_1)$. Alors $g_2^{-1} \star g_1 \in \ker(\varphi) = \{e\}$. Il en suit que $g_2^{-1} \star g_1 = e$, donc $g_1 = g_2$. Cela montre que φ est injectif. □

Définition 12.9. *Un homomorphisme de groupes qui est bijectif est appelé un* isomorphisme.
Parfois on appelle un homomorphisme injectif un monomorphisme *et un homomorphisme surjectif un* épimorphisme. *(Nous n'allons pas utiliser ces deux derniers termes.)*

Lemme 12.10. *Soient $(G, \star, e)$ et $(H, \circ, \epsilon)$ des groupes et $\varphi : (G, \star, e) \to (H, \circ, \epsilon)$ un isomorphisme de groupes. Comme φ est bijectif, il existe un inverse $\psi : H \to G$.*
Alors ψ est aussi un homomorphisme de groupes.

Démonstration. Soient $h_1, h_2 \in H$. Nous calculons :

$$\varphi(\psi(h_1) \star \psi(h_2)) = \varphi(\psi(h_1)) \circ \varphi(\psi(h_2)) = h_1 \circ h_2.$$

On applique ψ et obtient :

$$\psi(\varphi(\psi(h_1) \star \psi(h_2))) = \psi(h_1 \circ h_2),$$

donc $\psi(h_1) \star \psi(h_2) = \psi(h_1 \circ h_2)$ et on voit que ψ est un homomorphisme de groupes. □

Corollaire 12.11. *Soient G un groupe et $H_1, H_2 \leq G$ deux sous-groupes finis de G.*
Si $\mathrm{pgcd}(\#H_1, \#H_2) = 1$, alors $H_1 \cap H_2 = \{1\}$.

Démonstration. Soit $g \in H_1 \cap H_2$. Donc $\mathrm{ord}(g) \mid \#H_1$ et $\mathrm{ord}(g) \mid \#H_2$, donc $\mathrm{ord}(g) = 1 = \mathrm{pgcd}(\#H_1, \#H_2)$, donc $H_1 \cap H_2 = \{1\}$. □

Proposition 12.12 (Classification des groupes cycliques)**.** *Soit G un groupe cyclique.*

(a) Si $n = \#G$ est fini, alors G est isomorphe au groupe $(\mathbb{Z}/n\mathbb{Z}, +, \overline{0})$.

(Si on dit que deux groupes sont isomorphes, cela veut dire qu'il existe un isomorphisme de groupes entre les deux.)

(b) Si G n'est pas fini, alors G est isomorphe au groupe $(\mathbb{Z}, +, 0)$.

Démonstration. Soit g un générateur de G.
(a) L'application

$$\varphi : \mathbb{Z}/n\mathbb{Z} \to G, \quad \overline{a} \mapsto g^a$$

est bien définie et un isomorphisme de groupes. Effectivement, elle ne dépend pas du représentant a de la classe $\overline{a}$ modulo n car $g^{a+bn} = g^a(g^n)^b = g^a$. Elle est clairement un homomorphisme de groupes surjectif, donc bijective car le cardinal de $\mathbb{Z}/n\mathbb{Z}$ et de G est n.
(b) Comme G n'est pas fini, $\mathrm{ord}(g)$ n'est pas fini non plus. L'application

$$\varphi : \mathbb{Z} \to G, \quad a \mapsto g^a$$

est un isomorphisme de groupes. Effectivement, elle est clairement un homomorphisme de groupes surjectif. Si $g^a = g^b$ avec $a \neq b$, alors $g^{b-a} = 1$ donc g est d'ordre fini, contradiction. □

Proposition 12.13. *Soient G un groupe et $g \in G$ un élément d'ordre fini. Alors pour tout $i \in \mathbb{N}_{>0}$ on a*

$$\mathrm{ord}(g^i) = \frac{\mathrm{ppcm}(i, \mathrm{ord}(g))}{i} = \frac{\mathrm{ord}(g)}{\mathrm{pgcd}(i, \mathrm{ord}(g))}.$$

En particulier, si $i \mid \mathrm{ord}(g)$, alors $\mathrm{ord}(g^i) = \frac{\mathrm{ord}(g)}{i}$.

Démonstration. Comme $(g^i)^{\mathrm{ord}(g)} = (g^{\mathrm{ord}(g)})^i = 1$, il est clair que $\mathrm{ord}(g^i) < \infty$. Soit $m = \mathrm{ord}(g)$. On cherche le $n \geq 1$ minimal tel que

- $m \mid n$ ($\Leftrightarrow g^n = 1$) et
- $i \mid n$ ($\Leftrightarrow g^n = (g^i)^{n/i}$).

Donc, $n = \mathrm{ppcm}(m, i)$ et $\mathrm{ord}(g^i) = \frac{n}{i} = \frac{\mathrm{ppcm}(i,m)}{i} = \frac{\mathrm{ppcm}(i,m)\cdot\mathrm{pgcd}(i,m)}{i\cdot\mathrm{pgcd}(i,m)} = \frac{i\cdot m}{i\cdot\mathrm{pgcd}(i,m)} = \frac{m}{\mathrm{pgcd}(i,m)}$. □

Définition-Lemme 12.14. *Soit I un ensemble et pour tout i soit G_i un groupe. Alors le produit cartésien $\prod_{i\in I} G_i$ est un groupe, appelé* produit direct de G_i, $i \in I$, *pour la loi de groupe*

$$\cdot : \prod_{i\in I} G_i \times \prod_{i\in I} G_i \to \prod_{i\in I} G_i, \quad (g_i)_{i\in I} \cdot (h_i)_{i\in I} := (g_i \cdot h_i)_{i\in I}$$

et l'élément neutre $(1)_{i\in I}$.

Démonstration. Le cas $I = \{1, 2\}$ est un exercice. Le cas général marche de la même manière. □

Lemme 12.15. *Soient G un groupe abélien fini et $H_1, H_2 \leq G$ deux sous-groupes de G. Si $H_1 \cap H_2 = \{1\}$ (ce qui est le cas, en particulier, si $\mathrm{pgcd}(\#H_1, \#H_2) = 1$ par le corollaire 12.11), alors l'application $\phi : H_1 \times H_2 \to G$ donnée par $(h_1, h_2) \mapsto h_1 h_2$ est un homomorphisme de groupes injectif.*

Démonstration. **Homomorphisme** On calcule

$$\phi((h_1, h_2)(h_1', h_2')) = \phi((h_1 h_1', h_2 h_2')) = h_1 h_1' h_2 h_2' \overset{\text{abélien}}{=} h_1 h_2 h_1' h_2' = \phi((h_1, h_2))\phi((h_1', h_2')).$$

Injectivité $\phi((h_1, h_2)) = h_1 h_2 = 1$, donc $h_1 = h_2^{-1} \in H_1 \cap H_2 = \{1\}$, donc $h_1 = h_2 = 1$.

□

Exemple 12.16. *Nous faisons la liste de tous les groupes d'ordre ≤ 7 à isomorphisme près.*

- *Le seul groupe d'ordre 1 est le groupe trivial ; son seul élément est l'élément neutre.*
- $n = 2, 3, 5, 7$. *Comme tout groupe d'ordre premier est cyclique par le corollaire 11.11, il en suit que le seul groupe d'ordre n à isomorphisme près est $\mathbb{Z}/n\mathbb{Z}$.*
- $n = 4$ *: Nous connaissons deux groupes d'ordre 4 : $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ qui ne sont pas isomorphes (le premier est cyclique et le deuxième non-cyclique). On va démontrer qu'il n'y en a pas plus ; on verra notamment que tout groupe d'ordre 4 est abélien (c'était déjà un exercice).*

  Soit G un groupe d'ordre 4 qui n'est pas cyclique (s'il est cyclique, il est isomorphe à $\mathbb{Z}/4\mathbb{Z}$). On choisit $a \neq b$ deux éléments de G qui ne sont pas l'élément neutre. On a $\mathrm{ord}(a) \mid \#G$, donc $\mathrm{ord}(a) = 2$, car s'il était 4, le groupe serait cyclique engendré par a. Le même argument montre $\mathrm{ord}(b) = 2$. On a $\langle a\rangle \cap \langle b\rangle = \{1\}$. Soit $c := ab$. Il est clair que $c \neq 1, a, b$. Par le même argument $ba \neq 1, a, b$, donc $c = ba$. Donc G est abélien. Par le lemme 12.15 nous obtenons que $\langle a\rangle \times \langle b\rangle$ est isomorphe à G. Donc $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

- $n = 6$. *Nous connaissons deux groupes d'ordre* 6 *:* $\mathbb{Z}/6\mathbb{Z}$ *et* S_3 *qui ne sont pas isomorphes (par exemple : le premier est abélien et le deuxième non-abélien). On va démontrer qu'il n'y en a pas plus.*

  Soit G *un groupe d'ordre* 6 *qui n'est pas cyclique (s'il est cyclique, il est isomorphe à* $\mathbb{Z}/6\mathbb{Z}$*). Alors, tout élément* $1 \neq g \in G$ *doit être d'ordre* 2 *ou* 3 *car l'ordre doit être un diviseur de* $\#G = 6$ *et* $\mathrm{ord}(g) = 6$ *dirait que* G *est cyclique :* $\langle g \rangle = G$*.*

  On montre d'abord qu'il existe $a, b \in G$ *tels que* $\mathrm{ord}(a) = 3$ *et* $\mathrm{ord}(b) = 2$ *(cela est une conséquence directe du théorème de Sylow (que l'on verra plus tard)).*

  Supposons qu'il n'existe pas d'élément d'ordre 3*. Dans ce cas, tous les éléments non-neutres sont d'ordre* 2*. En conséquence* G *est abélien (par un exercice). Soient* $b_1 \neq b_2 \in G$ *deux éléments d'ordre* 2*. Alors, l'homomorphisme injectif* $\phi : \langle b_1 \rangle \times \langle b_2 \rangle \to G$ *du lemme 12.15 (noter :* $\langle b_1 \rangle \cap \langle b_2 \rangle = \{1\}$*) implique que l'image de* ϕ *est un sous-groupe d'ordre* 4*. Cela est une contradiction au corollaire 11.7. Donc, il existe* $a \in G$ *d'ordre* 3*.*

  On choisit $b \notin \langle a \rangle =: H$*. Comme* $G = H \sqcup bH$*, il en suit que* $b^2 \in H$ *ou* $b^2 \in bH$*. Le deuxième cas est impossible (sinon* b *serait dans* H*). Donc* $b^2 \in H$*. Donc* $\mathrm{ord}(b^2)$ *est* 1 *ou* 3 *(par la proposition 12.13). Le dernier cas mènerait à* $\mathrm{ord}(b) = 6$ *qui est exclu. Donc* $\mathrm{ord}(b) = 2$*.*

  Notons que $ab \neq 1, a, a^2, b$*. On a aussi* $a^2b \neq 1, a, a^2, b, ab$*. Donc* $G = \{1, a, a^2, b, ab, a^2b\}$*. Si* $ba = ab$*, alors* G *serait abélien et dans ce cas* $\mathrm{ord}(ab) = 6$ *(pour voir cela, il suffit de calculer* $ab \neq 1$*,* $(ab)^2 = a^2b^2 = a^2 \neq 1$ *et* $(ab)^3 = a^3b^3 = b^2b = b \neq 1$*) et le groupe serait cyclique ce que nous supposons ne pas être le cas. La seule autre possiblité est* $ba = a^2b$*.*

  Dans S_3 *nous posons* $A := (1\ \ 2\ \ 3)$ *et* $B := (1\ \ 2)$*. Nous définissons* $\phi : S_3 \to G$ *par* $\phi(\mathrm{id}) = 1$*,* $\phi(A) = a$*,* $\phi(A^2) = a^2$*,* $\phi(B) = b$*,* $\phi(AB) = ab$*, et* $\phi(A^2B) = a^2b$*. C'est clairement une bijection. Que c'est un homomorphisme est une conséquence de* $\mathrm{ord}(A) = 3$*,* $\mathrm{ord}(B) = 2$ *et* $BA = A^2B$ *qui est facilement vérifié.*